VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

POSOUZENÍ INFORMAČNÍHO SYSTÉMU FIRMY A NÁVRH ZMĚN
INFORMATION SYSTEM ASSESSMENT AND PROPOSAL OF ICT MODIFICATION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Stanislav Havlíček**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Lukáš Novák, Ph.D.**
SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Stanislav Havlíček**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Lukáš Novák, Ph.D.**
Akademický rok:	2020/21

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Posouzení informačního systému firmy a návrh změn

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současné situace
Vlastní návrhy řešení, přínos návrhů řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem je analyzovat stávající stav informačního systému vybrané organizace a jeho efektivnosti, posoudit tento stav a navrhnout změny směřující ke zlepšení stávajícího stavu a eliminaci nalezených rizik.

Základní literární prameny:

BASL, Josef a Roman BLAŽÍČEK. Podnikové informační systémy: podnik v informační společnosti. 3. aktualiz. a dopl. vyd. Praha: Grada, 2012. 323 s. ISBN 978-80-247-4307-3.

GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika. 2. přeprac. a aktualiz. vyd. Praha: Grada, 2009. 496 s. ISBN 978-80-247-2615-1.

MOLNÁR, Zdeněk. Efektivnost informačních systémů. 2. rozš. vyd. Praha: Ikar, 2000. 178 s. ISBN 80-247-0087-5.

SCHWALBE, Kathy. Řízení projektů v IT. Brno: Computer Press, 2007. 720 s. ISBN 978-80-251-1-26-8.

SODOMKA, Petr a Hana KLČOVÁ. Informační systémy v podnikové praxi. 2. aktualiz. a rozš. vyd. Brno: Computer Press, 2010. 501 s. ISBN 978-80-251-2878-7.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2020/21

V Brně dne 28.2.2021

L. S.

Mgr. Veronika Novotná, Ph.D. ředitel	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Diplomová práce zpracovává analýzu informačního systému základní školy a návrhu změn. Práce se skládá z tří částí, první část je o teorii, kterou je potřeba znát pro pochopení problematiky. Druhou částí je analýza informačního systému a samotné společnosti. Závěrečná část obsahuje návrh změn, které mají zlepšit fungování školy z pohledu informačních technologií.

Abstract

The diploma thesis processes analysis of information system of the primary school and proposal of modifications. The thesis consists of three parts, first part is about theory you need to know to understand the issue. The second part is the analysis of the informational system and the company itself. The final part contains a proposal of modifications to improve the functioning od the school in terms of information technologies.

Klíčová slova

Informační systém, informační technologie, Lewinův model změny, analýza rizik

Key words

Information system, information technology, Lewin’s model of change, risk analysis

Bibliografická citace

HAVLÍČEK, Stanislav. *Posouzení informačního systému firmy a návrh změn* [online]. Brno, 2021 [cit. 2021-05-16]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/133689. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Lukáš Novák.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 16.05.2021

_____

Bc. Stanislav Havlíček

Poděkování

Rád bych poděkoval panu Ing. Lukáši Novákovi, Ph.D., za uplynulé roky studia a následně rady se zpracováním bakalářské práce. Musím také poděkovat všem kolegům v práci za dodání podkladů pro vypracování některých kapitol. Závěrem nesmím zapomenout poděkovat své přítelkyni za její trpělivost se mnou během psané této práce.

OBSAH

ÚVOD

Tato diplomová práce je o analýze informačního systému soukromé základní školy v Brně a o návrhu změn ve fungování IT pro tuto firmu. Informační technologie jsou dnes všudypřítomné a pravděpodobně neexistuje úspěšná firma, která by nepoužívala informační systém využívající informační technologie. Společnosti, ale často podceňují význam průběžné údržby IT a po nákupu nové techniky a počátečním nastavení přestávají řešit provozní potřeby těchto zařízení. Řeší až vzniklý problém, jehož řešení je finančně i časově nákladnější než průběžná kontrola a údržba zařízení.

V první části práce se nachází teoretický základ, který je potřeba znát pro pochopení problematiky informačních systémů. Jedná se o vysvětlení základních pojmů, jak se dělí podnikové informační systémy a co jsou podnikové procesy nebo seznámení se s IS/ICT bezpečností. Poté se v teoretické části nachází popis různých analýz a modelů, které jsou poté použity v analytické nebo návrhové části.

Následující část se zabývá analýzou současné situace firmy pomocí analýz přestavených v teoretické části. Na analýzy firmy navazují analýzy informačního systému, které mají najít jeho slabá místa a odhalit nevhodně nastavené procesy. Důležitou částí jsou informace získané z rozhovorů se zaměstnanci firmy, kde je poznat odlišný pohled na celou problematiku.

Poslední částí diplomové práce je samotný návrh změn, které vycházení z odhalených nedostatků v analytické části. Tyto změny mají za cíl zlepšit vnitropodnikové procesy z pohledu bezpečnosti a efektivity.

VYMEZENÍ PROBLÉMU A CÍLE PRÁCE

Cílem práce je analyzovat současný stav informačního systému společnosti ScioŠkola Brno – základní škola s.r.o. Následně tento stav posoudit a navrhnout změny, které nasměrují společnost ke zlepšení stávajícího stavu převážně v oblasti bezpečnosti IT. Návrh změn má obsahovat analýzu rizik, aby se omezily možné problémy při realizování těchto změn.

Součástí analýzy aktuálního stavu je i názor zaměstnanců společnosti na spokojenost se školním informačním systémem a na fungování firemního IT, ať už z pohledu technického zázemí, tak názoru na IT procesy – řešení problémů.

1 TEORETICKÁ VÝCHODISKA PRÁCE

Tato část obsahuje teoretický základ pro celou diplomovou práci, popsání základních pojmů a vychází z ní použité analýzy na, které je navázáno v návrhu řešení.

1.1 Základní pojmy

Tato kapitola se zaměřuje na seznámení se s pojmy jako: data, informace, znalosti a systém. Se zaměřením na jejich rozdíly, jejich pochopení je nezbytné pro pochopení problematiky informačních systémů jako celku.

1.1.1 Data

Jedná se o fyzický záznam, ze kterého lze dekódováním získat informace. Dekódováním dat se rozumí například čtení zapsaného textu. Data je možné uchovávat na papíře nebo případně v elektronické podobě (na pevných discích nebo DVD), mohou se vyskytovat také ve formě elektrického signálu nebo elektromagnetického záření (při přenosu mezi zařízeními). (1)

1.1.2 Informace

Informaci lze porozumět jako vjemu splňující tři požadavky. Jedná se o syntaxi což je pochopení sdělení. Další je sémantika, která je o porozumění obsahu. Poslední částí je relevance, tedy že zpráva musí mít pro příjemce význam. (1)

Informace jsou tedy dekódovaná data, která pro uživatele mají určitý význam. Není možné je samostatně skladovat, lze je uchovávat pouze ve formě dat. (2)

1.1.3 Znalosti

Porozuměním informaci spolu s kombinací s dalšími informacemi se získává znalost. Pomocí znalostí se dekódují informace z dat a z těchto informací se následně získávají další znalosti. Díky znalostem se lze kvalitněji rozhodovat oproti náhodnému výběru z možností. Doba, během které vzniká rozhodnutí je omezena podle délky trvání problému, to znamená že nemá smysl uvažovat, jak nejlépe uhasit hořící elektronické zařízení, když hoří celá budova. (1)

1.1.4 Systém

Systémem podle teorie systémů je uspořádaná množina prvků, které jsou spolu provázány a jako celek mají určité vlastnosti. Pro zjišťování efektivnosti systému je možné použít pouze systémy s cílovým chováním, tzn. je tedy možné definovat jejich účel. Ve výsledku nestačí, aby všechny prvky fungovaly, protože je nutná i funkční spolupráce mezi nimi a změna v libovolném prvku ovlivní ostatní prvky systému. (2)

1.2 Informační systém

Není jednoznačná shoda na definici pojmu „informační systém“. Jedna z možných definic je: *„Informační systém je soubor lidí, technických prostředků a metod (programů), zabezpečujících sběr, přenos, zpracování, uchování dat, za účelem prezentace informací pro potřeby uživatelů činných v systémech řízení.“* (2) (3)

Informační systém je definován i ve standardu ISO/IEC 2382-1. V něm se píše o zpracování, poskytování a šíření informací, kde zdrojem informačního systému jsou lidé, technické a finanční zdroje. (4)

Jde o propojení těchto součástí do jednoho celku a součástí tohoto systému jsou také vazby mezi jednotlivými prvky. (1)

1.3 Podnikové informační systémy

Podnikový informační systém je tvořen lidmi, kteří zpracovávají podniková data. Výstupem tohoto zpracování je informační a znalostní báze, která je využita k řízení podnikových procesů a pomáhá manažerům organizace v rozhodování. (5)

Součástí podnikového informačního systému je spolu s lidmi i hardware a software, který pomáhá procesy, které zpracovávají podniková data, automatizovat. Jedná se o technologický pohled na podnikové informační systémy. (5)

Podnik lze rozdělit do několika organizačních úrovní, podle způsobu práce s informacemi a zároveň na jak velký časový interval se zaměřují. Jedná se o úrovně provozní, znalostní, řídící a strategickou. (5)

Provozní úroveň se zaměřuje na denní otázky typu: „Jaký je aktuální stav skladových zásob?“ Podnikový informační systém na této úrovni tedy musí dodat přesné a aktuální

informace. Tato úroveň je využívána zejména nižším managementem, případně běžnými pracovníky. (5)

Znalostní úroveň obsahuje například spokojenost zákazníků (zpětnou vazbu) s naší společností. Nejedná se tedy o okamžité údaje, ale o data sesbíraná za zvolené období. S těmito daty běžně pracuje management všech úrovní. (5)

Řídící úroveň dává odpověď spíše na dlouhodobé otázky, zda vše funguje podle plánu. Využívá ji tedy střední a vrcholový management, který na tyto otázky potřebuje znát odpověď. (5)

Nejvyšší úrovní je strategická, která dodává odpovědi na otázky v dlouhodobém časovém rozpětí (v řádu let). Jedná se o zjišťování trendu v následujících letech. Tato úroveň je nápomocná vrcholovému managementu organizace. (5)

Podnikový informační systém se dělí do několika podsystémů, které dohromady tvoří celopodnikový systém.

1.3.1 ERP systémy

Zkratka ERP pochází z anglického Enterprise Resource Planning (Plánování podnikových zdrojů). *„Informační systém kategorie ERP definujeme jako účinný nástroj, který je schopen pokrýt plánování a řízení hlavních interních podnikových procesů (zdrojů a jejich transformaci na výstupy), a to na všech úrovních, od operativní po strategickou.“* Hlavními interními podnikovými procesy se rozumí: výroba, nákup, prodej, vnitřní logistika, lidské zdroje a ekonomika. (5)

ERP systémy se dělí podle schopnosti zahrnout hlavní podnikové procesy. Systémy, které umí integrovat všechny výše zmíněné procesy se nazývají All-in-One. Jedná se o univerzální ERP systémy, které lze použít napříč obory a velikosti firem. Pro menší a středně velké firmy, bez netypických procesů jsou vhodné levnější a méně robustní systémy kategorie Lite ERP. Poslední možnou skupinou jsou Best-of-Breed systémy, které jsou zaměřené pro specifické obory nebo procesy. (5)

ERP systémy automatizují a integrují hlavní podnikové procesy, sdílejí data, postupy a standardizují je napříč celým podnikem, vytvářejí a zpřístupňují informace v reálném čase, mají schopnost zpracovávat historická data a mají celostní přístup k prosazování ERP koncepce. (5)

Z technologického pohledu se od ERP systémů vyžaduje výkonnost, spolehlivost a bezpečnost. Z toho plyne architektura server/klient. Výkonnost a spolehlivost se odvíjí od zvoleného hardwaru a softwaru. Bezpečnost závisí na splnění několika požadavků jako šifrovaní komunikace, nemožnost současné editace stejných záznamů různými uživateli, vytváření logu (záznamu) změn, autentizace, autorizace a správa uživatelů, možnost změny přístupových údajů uživatelem, možnost zpětné vazby mezi uživatelem a tvůrcem systému, monitoring chybových stavů kvůli usnadnění jejich nápravy. (5)

1.3.2 CRM systémy

Z anglického Customer Relationship Management neboli Řízení vztahů se zákazníky. Nejedná se o tzv. marketingový informační systém. CRM systémy mají dvě hlavní uplatnění, a to uspokojit potřeby zákazníků a řídit jejich ziskovost. Sjednocení a centralizování kontaktů a komunikace se zákazníkem je jedním z cílů CRM systémů. (5)

Na rozdíl od ERP systémů se CRM systémy zaměřují na externí podnikové procesy, které patří do obchodního cyklu. Obchodní cyklus zahrnuje řízení kontaktů, řízení obchodu, řízení marketingu a servisní služby. (5)

Při řízení vztahu se zákazníky existují dva principů – tahu a tlaku. Princip tahu znamená projev zájmu zákazníka a ten iniciuje kontakt (reklamace zboží). Principem tlaku se tady rozumí přesvědčování zákazníků podnikem o vhodnosti jejich nabídky (marketing). (5)

Z technologického pohledu lze CRM systémy dělit do tří částí: operační, kooperativní a analytickou. Operační část zahrnuje řízení obchodu tedy objednávkový cyklus, řízení marketingu a servis. Kooperativní část se zaměřuje na řízení kontaktů v rámci vícekanálové komunikace. Analytická část zahrnuje Business Intelligence (BI) a Customer Intelligence (CI). BI získává data z ostatních částí podnikového informačního systému a CI z ostatních částí CRM systému. Analytické CRM slouží k získání znalostí pro lepší cílení marketingu (zvýšení zisku) a udržení stávajících zákazníků například na základě zpětných vazeb. (5)

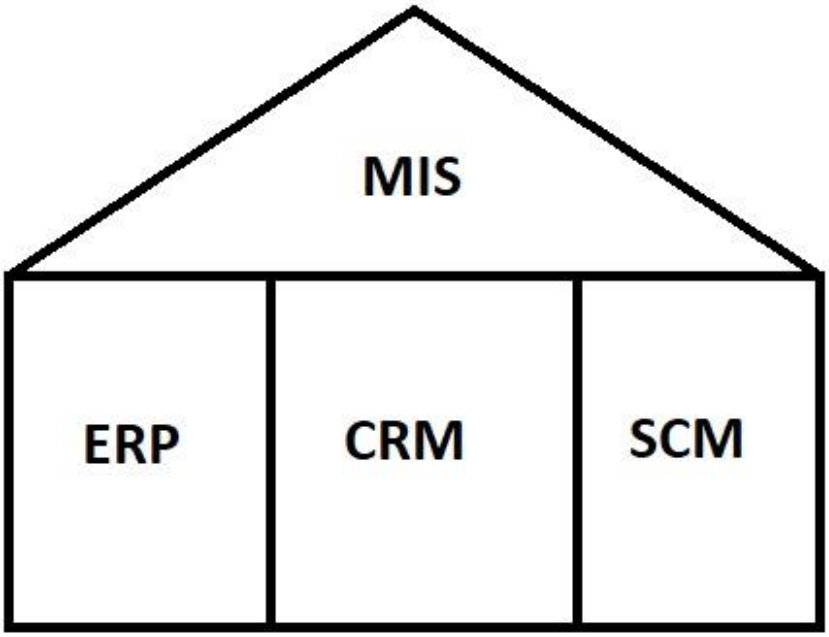
1.3.3 SCM systémy

SCM systémy neboli Supply Chain Management, v češtině Správa dodavatelského řetězce se zabývá vnější logistikou, zjednodušeně vztahem dodavatel-odběratel. Součástí je také strategické rozhodování o konkrétních dodavatelích, outsourcingu nebo

zákaznických požadavcích. Důležitou část SCM systému je také optimalizace procesů, která je možná díky provázanosti celého podnikového informačního systému. (5)

1.3.4 MIS systémy

Manažerský informační systém funguje jako podpora pro management v rozhodování. SCM dohromady s ERP a CRM tvoří základní kameny podnikového informačního systému a MIS je postaven na nich a zastřešuje je. Stejně jako analytická část CRM využívá Business Intelligence jako nástroje pro analýzu podnikových dat. Neslouží k podpoře pouze strategického rozhodování, ale také operativního, používá jej tedy celý management podniku. (5)



Obrázek 1 Schéma podnikového IS (vlastní zpracování dle (1))

1.3.5 Školní informační systémy

Školní informační systémy jsou specifickou částí manažerských informačních systémů. Tyto systémy se liší v datech, která uchovávají a poskytují uživatelům. Ve školních informačních systémech jsou uloženy údaje o žácích, zaměstnancích, klasifikace žáků, jejich vysvědčení, třídní knihy, rozvrhy, suplování a také data, která obvykle jsou uchována v dříve zmíněných částech IS, například soupis majetku školy nebo její rozpočet. (6)

Existuje mnoho různých informačních systémů pro školy, mezi nejznámější patří Bakaláři, Škola Online nebo Edookit. Kvalitně zvolený informační systém ve škole umožňuje efektivnější rozhodování pro vedení školy. Současně je nutné, aby byl systém správně nastaven podle požadavků školy a aby jeho uživatelé byli řádně proškoleni, jinak nebudou schopni využít jeho možností. (6)

1.4 Podnikové procesy

„Proces je soubor vzájemně souvisejících nebo vzájemně působících činností, které přeměňují vstupy na výstupy.“ Proces má několik základních charakteristik. Jsou jimi opakovatelnost, výstupem je produkt nebo služba s přidanou hodnotou, má měřitelné parametry, má vlastníka a zákazníka, je definován začátek, konec a návaznost na další procesy a využívá podnikové zdroje. (5)

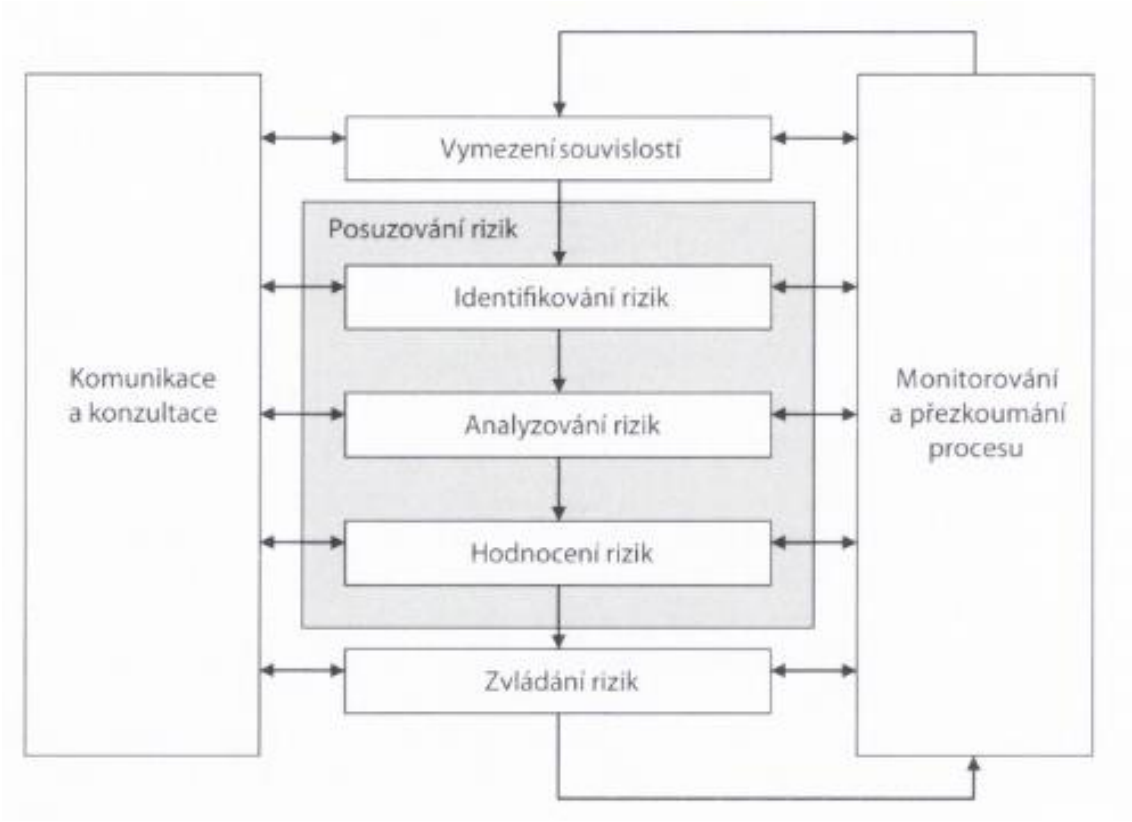
Každý proces patří do jedné ze tří kategorií. Buď se jedná o řídící proces, kam patří například strategické plánování nebo řízení inovací a kvality. Tyto procesy mají na starost rozvoj a řízení společnosti a podporují funkčnost ostatních procesů podniku. Druhou kategorií jsou hlavní procesy jako výroba, logistika, řízení vztahů se zákazníky. V rámci těchto procesů se vytváří hodnota ve formě výrobků nebo služeb pro externí zákazníky. Poslední skupinou procesů jsou podpůrné procesy, které zahrnují ekonomiku, HR oddělení, IT atd. Tato sada zajišťuje fungování ostatních procesů dodáváním hmotných i nehmotných výstupů. Podpůrné procesy nevytváří hodnotu pro podnik. (5)

Procesy jde také dělit z pohledu jejich vlastníka, což je role v podniku, která má na starost jeho řízení a optimalizaci. Procesy mohou být interní nebo externí. U interních procesů má management společnosti nad nimi kontrolu, a tedy i vlastníka. Jedná se o procesy ve výrobě, ekonomice nebo oddělení lidských zdrojů. Externí procesy nemají přesně definovaného vlastníka, protože je nemá plně pod kontrolou podnik, ale z části na ně mají vliv i dodavatelé nebo odběratelé (zákazníci). Jde o procesy patřící pod řízení vztahů se zákazníky nebo řízení dodavatelského řetězce. (5)

1.5 Řízení rizik

Jde o součást strategického řízení společnosti. Tento proces se skládá z pěti podprocesů. Jde o komunikaci a konzultaci, vymezení souvislostí, posuzování rizik, zvládání rizik a

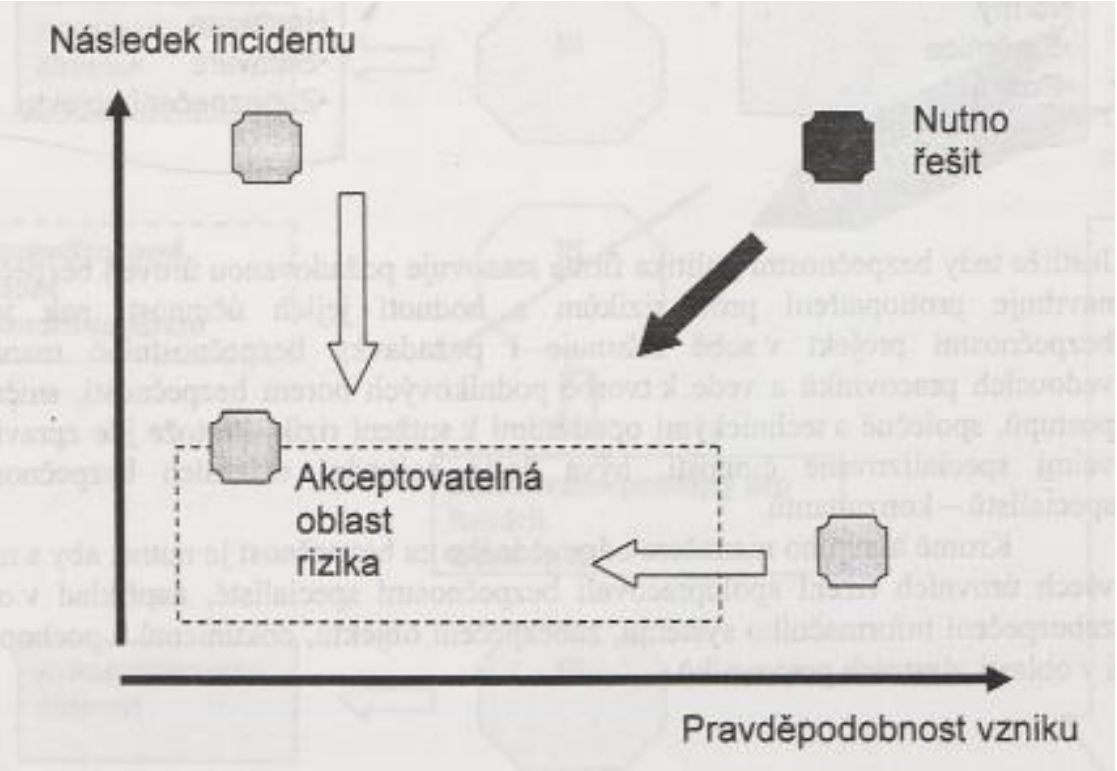
monitorování a přezkum procesu. Podproces posuzování rizik se dále dělí na identifikaci rizik, analýzu těchto rizik a jejich hodnocení. Řízení rizik je stále probíhající proces. (7)



Obrázek 2 Proces řízení rizika (7)

Subproces komunikace a konzultace vytváří plán pro tyto činnosti ve vztahu s interními a externími zainteresovanými stranami. Během vymezení souvislostí se definuje, co všechno řízení rizik zahrne. Identifikace rizik identifikuje, o která aktiva se jedná, jejich hodnotu a následně jaké existují pro tyto aktiva hrozby. Analýza rizik analyzuje tyto hrozby a stanovuje jejich pravděpodobnost vzniku, závažnost dopadu a následně úroveň rizika. Hodnocení rizik porovná úroveň rizika se stanovenými kritérii a rozhodne, zda je potřeba s konkrétními riziky dále pracovat. Zvládání rizik definuje, jak na jednotlivá rizika reagovat. Může se jednat o retenci (podstoupení) rizika, kdy se riziko přijme a není snaha jej snížit. Druhou možností je redukce rizika, kdy se buď sníží dopad rizika nebo se sníží pravděpodobnost jeho vzniku. Případně se může jednat o kombinaci obou. Třetí variantou je transfer rizika, kdy se riziko přesune na jiný subjekt, jde například o různé druhy pojištění. Poslední možností je vyhnutí se riziku, kdy se společnost zcela vyhne rizikové aktivitě. Poslední částí procesu je monitorování a přezkum rizika, které je

potřeba dělat pravidelně a získané podklady využít jako vstup pro začátek procesu řízení rizik. (7)



Obrázek 3 Hodnocení rizik (1)

1.5.1 Analýza rizik

Existují tři typy analýzy rizik. Kvalitativní analýza používá slovní hodnocení při popisování pravděpodobnosti výskytu a závažnosti dopadu. Semikvantitativní analýza se vyjadřuje pomocí předem definované číselné stupnice například od 1 do 10. Kvantitativní analýza používá reálné hodnoty, pravděpodobnost výskytu v procentech a závažnost dopadu ve finančních nákladech. Úroveň rizika se počítá jako součin závažnosti dopadu a pravděpodobnosti výskytu. (7)

1.6 Bezpečnost IS/ICT

Za bezpečný informační systém lze označit takový, který splňuje tři podmínky důvěrnosti, integrity a dostupnosti. Podmínka důvěrnosti znamená, že se k datům uloženým v systému dostane pouze autorizovaný uživatel (ten, který se tam smí dostat). Integrita zaručuje nemožnost editovat data neautorizovaným uživatelům. Poslední

podmínkou je dostupnost, která zajišťuje přístupnost služeb systému uživatelům v potřebný čas. (8)

Z výše uvedeného plyne nemožnost dokonale bezpečného IS, protože umístěním serveru s IS na izolované místo. Bez připojení do počítačové sítě se sice docílí velmi vysoké míry důvěrnosti a integrity, ale nebude téměř žádná dostupnost. Je tedy nutné přijít s kompromisem mezi těmito podmínkami. (1)

Nejčastější bezpečnostní incidenty vznikají díky samotným pracovníkům společnosti, která IS používá. Bezpečnost IS proto zahrnuje i školení uživatelů, pravidla pro jejich chování v IS a také zabezpečení budovy firmy proti neoprávněnému vstupu nežádoucích osob. (1)

V případě zaměstnanců firmy se jedná o interní hrozby, poté existují externí hrozby, mezi které lze zařadit například zloděje, hackery, počítačové viry nebo přírodní živly (požár, povodeň a jiné). (1)

Bezpečnost IS/ICT lze rozdělit na bezpečnostní politiku organizace a bezpečnost IS.

1.6.1 Bezpečnostní politika organizace

Výchozím krokem je studie bezpečnosti, která obsahuje analýzu současného stavu a směr dalšího postupu. Následuje analýza rizik, po níž je možné vytvořit bezpečnostní politiku organizace. V tomto dokumentu musí být definována aktiva, která mají být chráněna. Také v něm musí být uvedeno, kdo za ně ponese odpovědnost, kdy tato opatření budou efektivní, jak se jejich dodržování bude kontrolovat a kdy a jak budou opatření realizována. Součástí bezpečnostní politiky organizace musí být reakce na možné incidenty, aby se předešlo chaotickému jednání, které bývá finančně dražší. (1)

Nejedná se o jednorázově vytvořený dokument, ale o stále probíhající proces, kdy na vytvoření (úpravu) bezpečnostních politik navazuje jejich kritické hodnocení a opětovná aktualizace podle nového výchozího stavu. (1)

1.6.2 Bezpečnost IS

Existuje pět základních bezpečnostních prvků, které chrání informační systémy společnosti. (1)

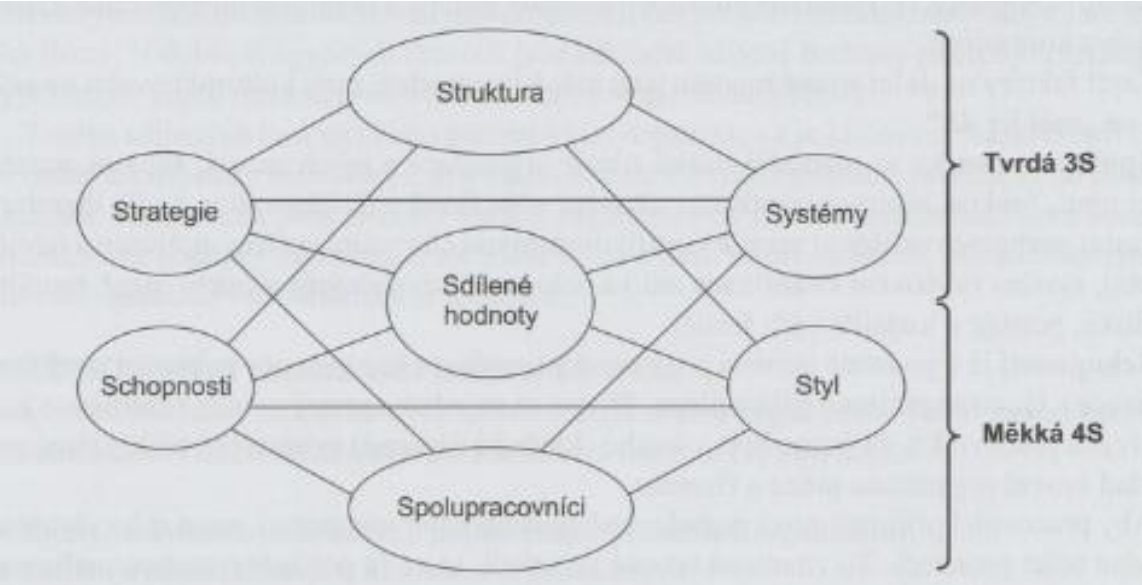
Prvním z nich je fyzická bezpečnost, která chrání před neoprávněným fyzickým přístupem, jedná se například o zámky, alarmy, bezpečnostní kamery atd. Pro případ výpadku elektrické energie, kterou bývá IS napájen je potřeba mít zajištěn záložní zdroj energie. Může se jednat o UPS (pro krátkodobý výpadek v řádu minut) nebo náhradní generátor. Je také potřeba mít vhodně nastavená přístupová práva uživatelů, aby se do IS dostali pouze oprávnění uživatelé a pouze do oprávněných částí. Součástí tohoto prvku je také firemní politika správy hesel. Čtvrtou částí je firewall, který může fungovat jako fyzické zařízení nebo jako program. Jedná se o nepostradatelnou součást ochrany nejen IS v nejrozšířenější počítačové síti – internetu. Posledním prvkem je antivir, který má za úkol chránit zařízení před počítačovými viry, což jsou jedny z nejčastějších útoků na informační systémy. (1)

Počítačové viry jsou programy, které mívají schopnost se šířit, ale hlavně působí škodu v zasaženém systému. Je mnoho různých druhů, které mají různý účel, může se jednat o zašifrování dat na disku a následné vydírání, odeslání dat bez vědomí uživatele, smazání dat, zpřístupnění bezpečnostní díry v zařízení pro další útok, využití výkonu zařízení pro potřeby útočníka nebo pro nežádoucí reklamy. (1)

Pravidelné zálohování dat je účinnou ochranou před poškozením nebo smazáním dat. Je potřeba mít zvoleno na které médium zálohu provádět (HDD, DVD, cloud …), kdy tyto zálohy fyzicky uložit a jak často zálohovat. Měly by existovat minimálně dvě kopie záloh, na odlišných médiích a v různých fyzických lokalitách, tato místa by se měla lišit od původního zdroje dat. (1)

1.7 McKinsey 7S

Jedná se o analýzu vnitřního prostředí společnosti. Jde o model firmy rozdělený do sedmi faktorů, které všechny začínají na písmeno S. Těmito faktory jsou: struktura, strategie, systémy, sdílené hodnoty, schopnosti, styl a spolupracovníci. První tři se označují jako „tvrdá 3S“ a zbylé čtyři jako „měkká 4S“. Důvodem pro toto rozdělení je horší hmatatelnost měkkých S. (9)



Obrázek 4 McKinsey 7S (9)

Strategie je o schopnosti společnosti naplňovat svou vizi a jak dokáže reagovat na hrozby a příležitosti v oboru. (9)

Struktura popisuje, jaké je organizační uspořádání uvnitř firmy. Možnými strukturami jsou například hierarchická, maticová, decentralizovaná nebo síťová. (9)

Systémy se věnují všem typům informačních systémů, které se ve společnosti používají (ERP, SCM, MIS a další). (9)

Spolupracovníci jsou všichni zaměstnanci firmy a také jejich znalosti, kvalifikace, funkce, role, motivace, loajalita a mnoho dalšího. (9)

Schopnosti nejsou pouze suma schopností jednotlivých spolupracovníků, ale jsou zde zahrnuty například i organizace práce nebo způsob řízení. (9)

Styl vyjadřuje způsob řízení společnosti managementem. Může se jednat například o direktivní (autokratický) styl nebo samořídící. (9)

Na sdílených hodnotách ve firmě by měla být shoda mezi vizí společnosti a názory, principy a idejemi spolupracovníků. (9)

1.8 Porterova analýza

Jde o analýzu oborového okolí organizace, která se skládá z pěti částí. Z vlivu dodavatelů a odběratelů, rizika vstupu nové konkurence, hrozby substitutů a z analýzy stávající konkurence. (9)

Obrázek 5 Porterova analýza (9)

Vliv dodavatelů závisí na odpovědi na následující otázky: jaká je nahraditelnost dodavatele, zda existuje konkurenční dodavatel, jak důležité pro podnikání jsou dodávané výrobky nebo služby a jak důležitým odběratelem pro dodavatele je společnost. (9)

Vliv odběratelů se odvíjí od jejich závislosti na produktu společnosti. Udává, zda v oboru existuje konkurence, případně jestli se jedná o několik malých odběratelů (například koncoví zákazníci v maloobchodě) nebo o jednoho významného odběratele (jiná firma – například mléko od farmáře pro výrobce másla). (9)

Riziko vstupu nové konkurence se odvíjí od náročnosti vstupu na trh (finanční, legislativní), prostoru na trhu (vyšší poptávka než nabídka), loajalita zákazníků a na odlišnosti výrobků na trhu. (9)

Hrozba substitutů je o existenci podobných produktů, jejich cenách, jak moc se tyto produkty liší a o jejich kvalitě. (9)

Stávající konkurence popisuje, kolik a jakých konkurentů se na trhu nachází. V čem se tito konkurenti liší, jakou část trhu zabírají, jestli mezi konkurencí existuje rivalita, jaká je spokojenost jejich zaměstnanců, případně jaké jsou jejich produkty atd. (9)

1.9 SLEPTE analýza

SLEPTE analýza je analýza faktorů vnějšího prostředí firmy, jedná se o soubor sociálních, legislativních, ekonomických, politických, technologických a ekologických částí. Lze se setkal s několika různými názvy pro tuto analýzu například PEST, PESTLE nebo SLEPT. Někdy se zde nenachází ekologické faktory nebo jsou politické a legislativní sloučeny do jednoho. (9)

Sociální faktory popisují různé demografické statistiky o populaci, makroekonomické údaje z trhu práce i kulturní nebo pracovní zvyklosti ve zvoleném prostředí (stát, kontinent, město apod.). (7)

Legislativní faktory se zabývají různými zákony, normami a vyhláškami v určené oblasti. Konkrétně se může jednat o daňové nebo antimonopolní zákony, zákony o účetnictví nebo občanský zákoník, případně i nadřazené nařízení jako GDPR, které platí v celé Evropské unii. (9)

Do ekonomických faktorů se řadí makroekonomické veličiny jako inflace nebo vývoj hrubého domácího produktu. Vliv má také centrální banka, která určuje úrokové sazby pro komerční banky a má vliv na směnný kurz domácí měny. (9)

K politickým faktorům se uvádí hodnocení politické stability, názory a vliv politických stran, postoj vůči státním vs. privátním podnikům nebo investicím. Také je nutné analyzovat i politické okolí státu, zda je součástí většího celku (EU, NATO…). (7)

V technologických faktorech se soustředí data o technologických trendech ve společnosti, kolik peněz je investováno do výzkumu a vývoje, jaké technologické produkty jsou na trhu k dostání a zda jsou lidé, kteří s nimi umí zacházet. (9)

Posledním faktorem je ekologický, který popisuje, jaké jsou ekologické podmínky v požadované lokalitě, které firmu mohou ovlivnit. Jde o požadavky na udržitelný rozvoj, obnovitelné zdroje energie a celkově ochranu životního prostředí. (9)

1.10 SWOT analýza

SWOT analýza zpracovává výsledky z ostatních analýz a vyhodnocuje silné (strengths) a slabé (weaknesses) stránky, spolu s příležitostmi (opportunities) a hrozbami (threats) společnosti. Silné a slabé stránky vychází z vnitřních analýz a jde například o dostatek nebo nedostatek zkušeností. Příležitosti a hrozby jsou výsledkem vyhodnocení vnějších analýz a může se jednat například o rostoucí trh (příležitost) nebo o rychle rostoucí konkurenční společnost (hrozba). (10)

Výsledkem této analýzy může být návrh nových projektů, které budou zaměřeny na zmírnění slabých stránek nebo hrozeb firmy, na posílení silných stránek nebo na využití příležitostí, případně na kombinaci několika z uvedených. (10)

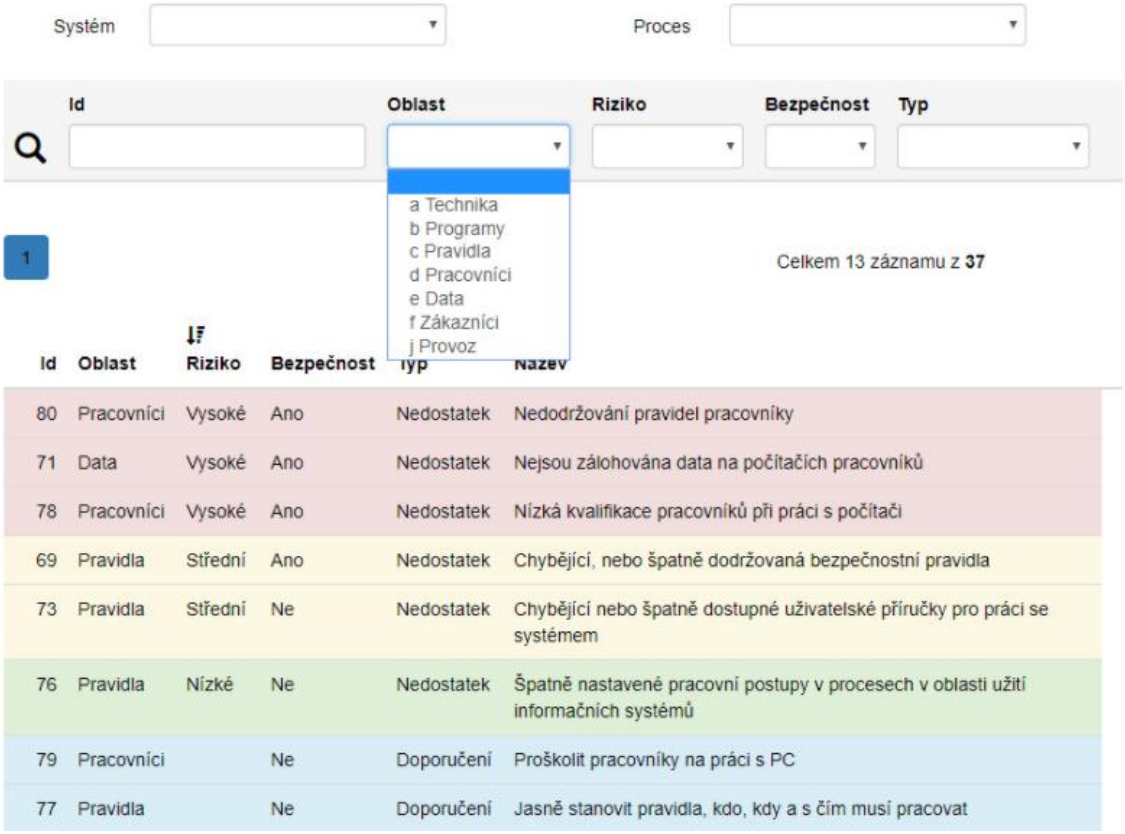
1.11 Zefis – audit IS

Tato služba se nachází na webovém portálu www.zefis.cz. Jedná se o elektronického konzultanta, který nabízí pomoc s hledáním nedostatků v informačním systému podniku, včetně oblasti bezpečnosti. Dodá také doporučení, jak tyto nedostatky zmírnit a zobrazí i porovnání s ostatními společnostmi v oboru. (11)

Systém Zefis získá data na základě vyplnění několika dotazníků. Z odpovědí a souvislostí mezi nimi vznikne přehledný soupis nedostatků dotazovaného podnikového informačního systému. Spolu se soupisem nedostatků dodá také seznam doporučení, jak lze tyto nedostatky odstranit. (11)

Portál tyto nedostatky dělí do sedmi skupin, kterým říká oblasti. Jsou jimi technika, programy, pravidla, pracovníci, data, zákazníci a provoz. Technika obsahuje veškerý hardware, který informační systém využívá. Oblast programů zahrnuje veškerý software, který se ve společnosti používá. Pravidla se zabývají firemními politikami, směrnicemi a pracovními postupy, jejich existencí, dodržováním a kontrolou. Ve skupině pracovníci se analyzují schopnosti zaměstnanců pracovat podle firemních politik a bez zbytečných chyb. V datech se jedná o jejich dostupnost, celistvost a důvěrnost. Oblast zákazníci se zabývá funkčním vztahem zákazníků podniku a podnikového informačního systémů. Poslední část provoz se zaměřuje na problémy vznikající během práce a na jejich řešení. Zjištěné nedostatky lze v seznamu rozkliknout a získat detailnější soupis informací. Tato

stránka umožňuje porovnání s ostatními podniky ve zvoleném odvětví a velikosti u zvoleného nedostatku. (11)



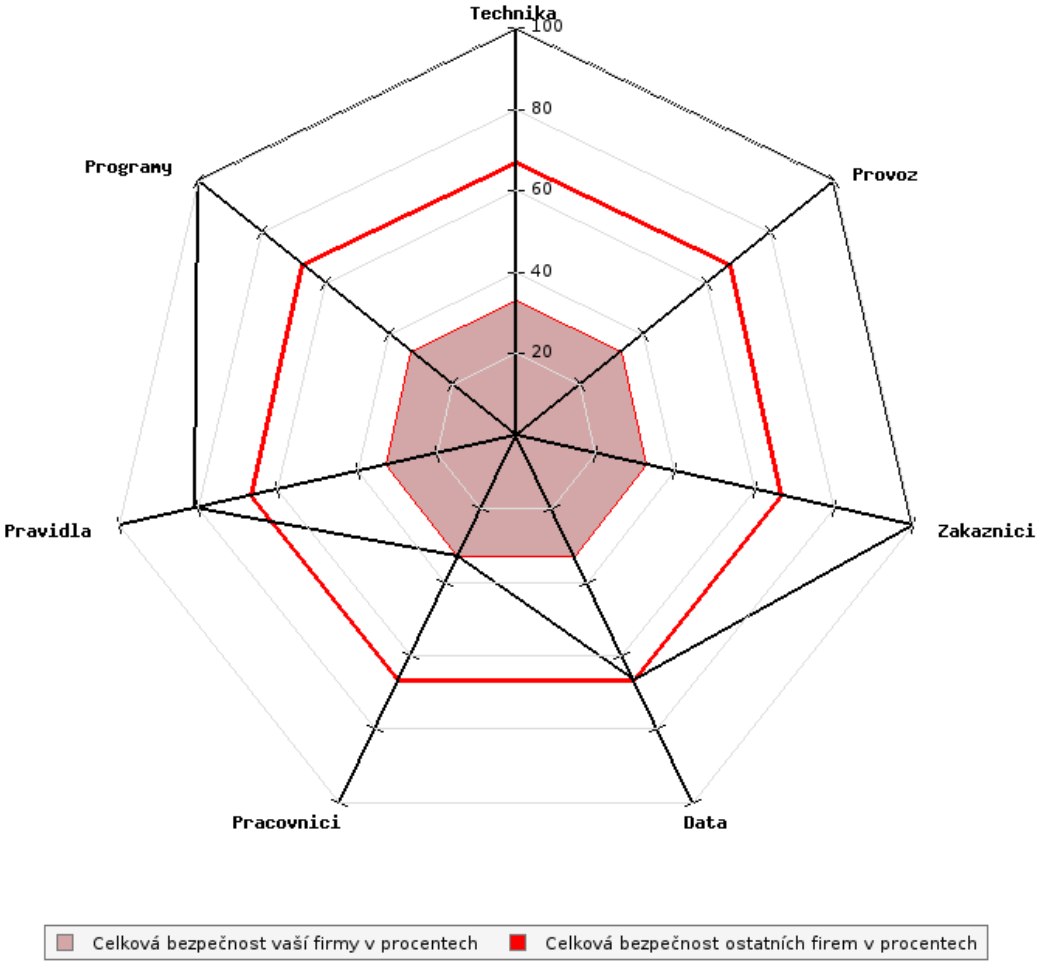
Obrázek 6 Portál Zefis – seznam nedostatků (11)

Zefis nezkoumá efektivitu informačního systému, protože vyžaduje příliš mnoho citlivých, převážně finančních dat. Efektivita systému neboli účinnost se počítá jako poměr přínosů k nákladům a u informačních systémů se nejedná o snadný výpočet. Informační systémy totiž mají také nevyčíslitelné (obtížně vyčíslitelné) přínosy. (11)

Pojmy efektivita a efektivnost se liší, v případě efektivnosti se jedná o stupeň dosažení stanoveného cíle. V podnikových informačních systémech se jedná o korektní výběr, nastavení a provozování informačního systému a o vhodně nastavených procesech. Maximální efektivnost je 100 %, ale ta se v reálných případech téměř nevyskytuje. (11)

Další oblastí, které se systém Zefis věnuje je bezpečnost. Její hodnotu vyjadřuje podle nalezených nedostatků. (11)

Efektivnost i bezpečnost portál zobrazí ve dvou paprskových grafech, kde zobrazená výsledná hodnota se rovná hodnotě nejslabší oblasti. Zároveň je z grafu vidět srovnání s ostatními společnostmi. (11)



Obrázek 7 Portál Zefis – graf efektivnosti bezpečnosti (11)

1.12 Kvalitativní výzkum

Na rozdíl od kvantitativního výzkumu, který spoléhá na přesná data, je kvalitativní výzkum více obecný, časově náročnější a umožňuje lepší pochopení problému, kterému se věnuje. (12)

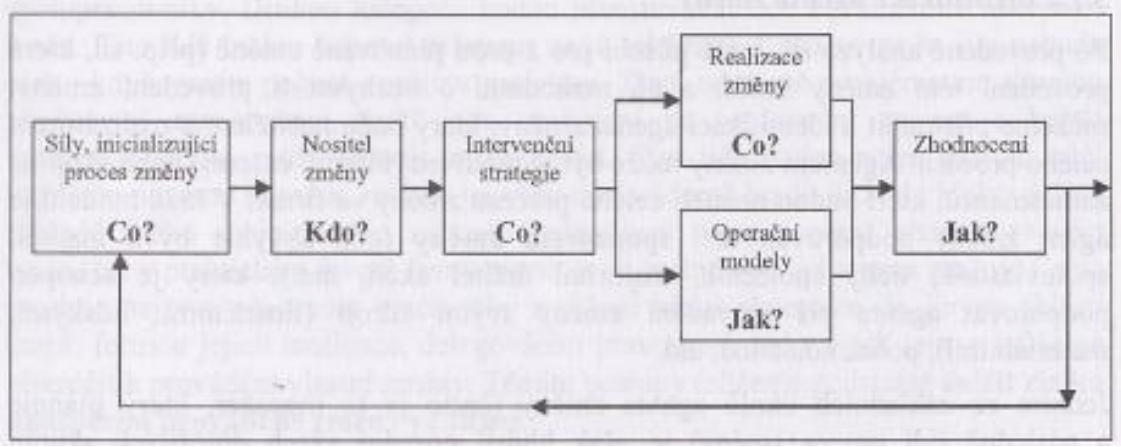
Existuje několik metod získávání dat do kvalitativního výzkumu. Jedná se o pozorování, čtení textů a dokumentů, rozhovory s účastníky výzkumu, poslech zvukových záznamů a sledování videozáznamů. (12)

Nevýhodou tohoto výzkumu je jeho obtížná opakovatelnost za dosažení stejných výsledků, protože odpovědi různých účastníků budou odlišné. Výsledky také mohou být snadno ovlivněny názorem výzkumníka. (12)

Kvalitativní výzkum je výhodné použít tam, kde nestačí hodnocení čísly a je potřeba podrobný popis. Je vhodný pro analýzu procesů, kdy číselné ohodnocení od dotazovaného neřekne, s čím je (ne)spokojen. (12)

1.13 Lewinův model

Lewinův model se používá k namodelování řízené změny ve firmě, která má za cíl zvýšit úroveň produktivity, zisku, bezpečnosti atd. Jaký je proces této změny je vidět na následujícím obrázku. (13)



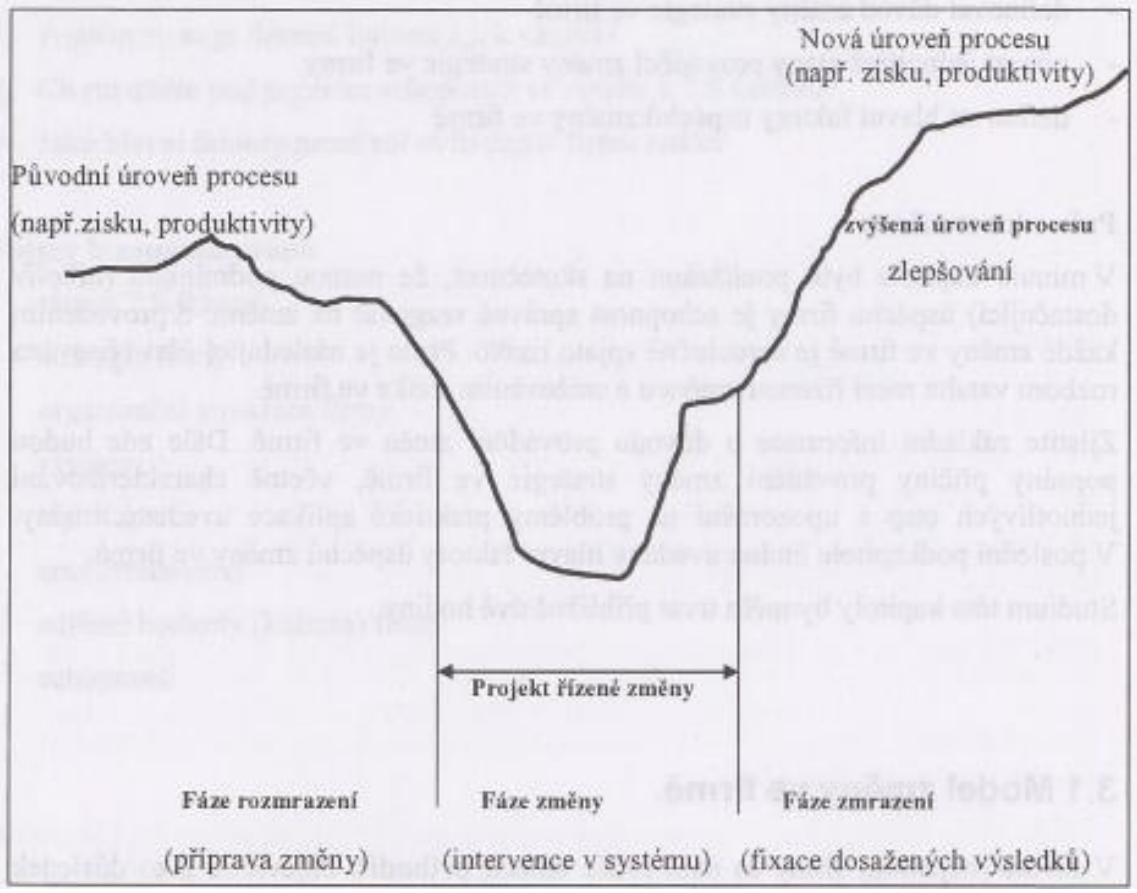
Obrázek 8 Lewinův model změny (13)

Nejprve je potřeba vědět co, kdo a jak působí tlak na změnu a jaký je očekávaný stav v budoucnu. Dále je potřeba zjistit kdo, kde a jak tuto změnu provede. A poslední otázkou je zhodnocení, jak proces změny dopadl. (13)

Osoba nebo skupina, která změnu realizuje se nazývá agent změny. Další důležitou rolí v Lewinově modelu je sponzor změny, což je osoba, která podporuje agenta během provádění změny svými zdroji nebo vlivem. Poslední rolí je advokát změny, což je jednotlivec nebo skupina, který změnu podporuje, ale nemá pravomoci ani odpovědnost k provedení této změny. (13)

Dalším krokem je identifikování intervenčních oblastí, které zasáhne plánovaná změna. Obvykle se jedná o lidské zdroje a jejich řízení, organizační strukturu firmy, technologie firmy, komunikační a organizační toky a procesy firmy. (13)

Proces změny se dělí na tři fáze. První částí je fáze rozmrazení, kde se připravují změny. Druhá část je fáze změny, kdy probíhají samotné řízené změny v systému. Poslední částí je fáze zmrazení, kdy se analyzuje výsledek těchto změn a očekává se zlepšení úrovně produktivity, zisku, bezpečnosti nebo jiných sledovaných parametrů. (13)



Obrázek 9 Fáze procesu změny (13)

1.14 Časová analýza PERT

Jedná se o techniku pro řízení časové náročnosti projektu, která se od metody CPM (metoda kritické cesty) liší v určování odhadu času na dobu trvání činnosti. Počítá se s váženým průměrem, kde výsledná hodnota (t) se rovná součtu optimistického odhadu (a), čtyřnásobkem nejpravděpodobnějšího odhadu (m) a pesimistickým odhadem (b), celý tento součet se poté vydělí šesti. (10)

$$ò_{سي} \frac{ώ_{طى} \tau_{عي} \acute{\alpha}_{طى} \tilde{ώ}_{طى}}{\varphi}$$

Rovnice 1 Vážený průměr v PERT (10)

2 ANALÝZA PROBLÉMU A SOUČASNÉ SITUACE

Tato část obsahuje seznámení se se společností a také zahrnuje analýzy 7S, SLEPTE, Porterovu a SWOT, které ohodnotí současný stav firmy. Následuje představení podnikového informačního systému a jeho zhodnocení pomocí analýz SWOT a Zefis. Součástí kapitoly jsou také informace získaná během rozhovorů s různými uživateli IS. Všechny tyto analýzy budou vstupními parametry pro vlastní návrhy řešení.

2.1 ScioŠkola Brno – základní škola, s.r.o.

ScioŠkola Brno – základní škola, s.r.o. je soukromá škola se sídlem na adrese Sokolova 145/4 v Brně v městské části Horní Heršpice. Zřizovatelem a vlastníkem ScioŠkoly Brno je společnost www.scio.cz, s.r.o. Škola byla zapsána do obchodního rejstříku 3. února 2016 a 1. září stejného roku, zde začala výuka. (14)

Z necelých 50 žáků se postupně rozšířila až na dnešních téměř 120 žáků a zájem nepolevuje. I z tohoto důvodu nedávno skončila rekonstrukce budovy a přístavba dalšího patra. Škola má v současnosti přibližně 27 zaměstnanců, a to převážně učitelů („průvodců“), asistentů pedagoga nebo družinářů („klubáků“ nebo „průvodců v klubu“). Mnoho ze zaměstnanců pracuje na různé varianty zkrácených úvazků. (15)

Celkem je v Česku 12 ScioŠkol, z toho jedna střední a ostatní základní. Všechny tyto školy mají společné principy, kterými se řídí. Chtějí vést ke svobodě a zodpovědnosti, kladou důraz na rozvoj kompetencí, inspirují, podporují, stimulují, učí vzájemnému respektu. Neškatulkují a mají individuální přístup podle potřeb jednotlivce, jsou partnerem pro školáky, tak i pro rodiče a ve výuce propojují školu s každodenním životem. (16)

2.1.1 SLEPTE analýza ScioŠkoly

Jedná se o analýzu okolí brněnské ScioŠkoly z pohledu sociálního, legislativního, ekonomického, politického, technologického a ekologického.

2.1.1.1 Sociální faktory

Počet obyvatel Brna je stálý, přibližně 377 tisíc. Stejně jako počty nově narozených, kterých se v obci narodí každý rok v průměru 4515, jde o průměr za roky 2010 až 2019.

V posledních 4 letech je počet narozených mírně vyšší, podobně rostou i počty přistěhování do města. (17)

V Brně se nachází Pedagogická fakulta Masarykovy univerzity, kde aktuálně studuje 4471 studentů. (18)

2.1.1.2 Legislativní faktory

Škola samozřejmě musí dodržovat všechny zákony, vyhlášky a nařízení vlády, které se jich týkají. Zejména se jedná o Školský zákon č. 561/2004 Sb., který upravuje vzdělávání ve školách, stanovuje podmínky tohoto vzdělávání a vymezuje práva a povinnosti osob, které ve vzdělávání působí. Jedná se o zaměstnance škol, žáky a jejich zákonné zástupce. (19)

V dnešní době je také potřeba dodržovat různá nařízení, která vznikla kvůli onemocnění covid-19. Tyto nařízení se vztahují na školská zařízení, jedná se například o povinné testování žáků i zaměstnanců, nošení roušek atd. Případně povinnost distanční (online) výuky u 2. stupně ZŠ nebo tzv. „rotační“ výuky v případě 1. stupně základních škol. (20)

Tím že se jedná o soukromou školu, tak je také nutné se řídit zákony, kterými by se měli řídit všichni podnikatelé na území České republiky, konkrétně Zákon č. 90/2012 Sb. o obchodních společnostech a družstvech, Zákon č. 563/1991 Sb. o účetnictví nebo například Zákon č. 262/2006 Sb., tedy zákoník práce a další. (19)

2.1.1.3 Ekonomické faktory

V Česku je vzdělání ve státních školách až na výjimky (například překročení běžné délky studia u vysokých škol) studium bezplatné. Proto existuje méně než desetina soukromých škol, oproti množství státních škol, které mohou být zpoplatněny. (17)

I přes zpomalení meziročního růstu průměrných mezd v druhém kvartálu roku 2020, tak průměrné mzdy neustále rostou a školství není výjimkou. (17)

2.1.1.4 Politické faktory

Politická situace je v Česku dlouhodobě stabilní a v oblasti vzdělání existuje shoda ve věci upravení strategie. Neexistuje ale shoda napříč politickým spektrem, jak strategii změnit. Příkladem může být postup u státní maturity z matematiky, kde se více než 10 let stále přichází s různými reformami. (20)

Je ale potřeba neustále sledovat změny hlavně v daňových zákonech a v platech učitelů. Růst učitelských platů je jedno z témat, kterému se věnují všechny politické strany. (21)

2.1.1.5 Technologické faktory

Kvůli pandemii onemocnění covid-19 se ve školství začalo více investovat do ICT techniky, která je potřebná pro distanční způsob výuky. Tyto investice mířily do nákupu notebooků a tabletů. Nová technika je určená pro vyučující a případně žáky z nemajetných rodin. V rámci této podpory nebylo možné investovat do nepřenosných PC nebo serverů, které by ale také mohly zlepšit distanční formu výuky. (20)

2.1.1.6 Ekologické faktory

Ve vzdělání nejsou ekologické regulace, ale může být tlak rodičů, aby byli jejich potomci vedeni k ekologickému smýšlení i ve své škole.

2.1.2 Analýza 7S ScioŠkoly

Analýza 7S se týká vnitřního fungování brněnské ScioŠkoly z pohledu sedmi oblastí: strategie, struktury organizace, systémů, stylu řízení, spolupracovníků, schopností a sdílených hodnot.

2.1.2.1 Strategie

Všechny ScioŠkoly mají společné principy, kterými se řídí. Chtějí vést ke svobodě a zodpovědnosti, kladou důraz na rozvoj kompetencí, inspirují, podporují, stimulují, učí vzájemnému respektu. Neškatulkují a mají individuální přístup podle potřeb jednotlivce. ScioŠkoly jsou partnerem pro školáky i pro rodiče a ve výuce propojují školu s každodenním životem. (16)

2.1.2.2 Struktura organizace

Ve škole funguje liniově-štábní struktura, kdy existuje ředitel školy a jeho zástupce, kteří jsou nadřazeni ostatním, ale zároveň například IT konzultant má jako nadřazený útvar všechny vyučující, ale zároveň i ředitele školy. Jedná se o kombinací liniové a funkcionální struktury, podle toho, o kterého zaměstnance se jedná.

2.1.2.3 Systémy

Škola na svých počítačích používá Windows 10, případně na pár zařízeních i Fedoru 32. Jako školský informační systém využívá produkt Edookit a pro účetnictví systém Pohoda. V komunikaci je možné používat dle osobních preferencí – maily, telefony, Edookit a vzhledem k probíhající epidemii nově také Google Meet.

2.1.2.4 Styl řízení

Vedení školy používá demokratický styl řízení, kdy se očekává zapojení všech zaměstnanců, kterých se rozhodnutí týká.

2.1.2.5 Spolupracovníci

Jedním ze základních předpokladů při výběru nových spolupracovníků je podobný žebříček hodnot, který škola vyučuje (viz strategie). Díky tomu mezi kolegy vládne přátelská atmosféra.

2.1.2.6 Schopnosti

Ve ScioŠkole se každý vyučující věnuje své oblasti zájmu, ve které vyniká nejvíce a nestává se, aby pracovník vyučující český jazyk zasahoval do práce kantora vyučujícího matematiku, a naopak. Zároveň ale je běžné, že během výuky matematiky je češtinář přítomný, aby díky svému odlišnému pohledu mohl látku vysvětlit jinak. Díky existenci školného je možné tyto zaměstnance ohodnotit odpovídajícím způsobem.

2.1.2.7 Sdílené hodnoty

Všechny ScioŠkoly sdílejí stejné hodnoty. Těmi jsou optimismus, odvaha, otevřenost, svoboda, morálka a aktivita. (16)

2.1.3 Porterova analýza

Porterův model pěti sil v prostředí ScioŠkoly Brno popisuje konkurenční prostředí a zahrnuje vliv dodavatelů a odběratelů, substituční produkty, stávající konkurenci a hrozbu nové konkurence.

2.1.3.1 Vyjednávací síla dodavatelů

Společnost má pouze jednoho významného dodavatele, tím je městská část Brno-Jih, která je vlastníkem budovy, kde ScioŠkola sídlí. Nedávno byla podepsána nová smlouva o nájmu budovy na 10 let a vliv tohoto dodavatele je střední.

Nákup pomůcek nebo techniky nemá pevného dodavatele, a například ISP byl před pár lety vyměněn. Všichni tito dodavatelé tedy mají nízkou vyjednávací sílu.

2.1.3.2 Vyjednávací síla zákazníků

Je otázkou, zda jsou firemními zákazníky žáci nebo jejich rodiče, ale protože školné platí rodiče, lze za zákazníky označit spíše právě rodiče. Změnit školu není extrémně náročné, zvláště když existují bezplatné alternativy. Zákazníci tak očekávají, že jim škola vyjde vstříc. Rodiče jako zákazníci mají vysokou vyjednávací sílu.

2.1.3.3 Hrozba substitučních produktů

Substitučním produktem k základnímu vzdělání ve škole je pouze domácí vzdělávání, které ale není příliš rozšířené, a navíc je finančně náročnější než školní docházka. Proto se jedná o nízkou hrozbu.

2.1.3.4 Hrozba nové konkurence

Kvůli vyšším finančním bariérám pro vstup na trh a potřebě zápisu nové školy do školského rejstříku a vysoké konkurenci nevznikají nové školy pořád. Navzdory tomu se pomalu prosazují alternativně zaměřené školy, právě kvůli rostoucí poptávce po nestátních školách nebo jiných výukových metodách. Hrozba nové konkurence má střední hodnotu.

2.1.3.5 Hrozba stávající konkurence

Jen v Brně se nachází 98 základních škol z toho 18 je zřízeno soukromým sektorem. Spolu s vysokou vyjednávací silou zákazníků je i hrozba ze strany stávající konkurence vysoká. (20)

2.1.4 SWOT analýza ScioŠkoly

Tato kapitola obsahuje vyhodnocení předchozích analýz v silných a slabých stránkách ScioŠkoly a jejích příležitostech a hrozbách.

2.1.4.1 Silné stránky

Mezi silné stránky brněnské ScioŠkoly patří odlišnost od její konkurence, výborná lokalita firmy a důraz na pro-zákaznický přístup.

2.1.4.2 Slabé stránky

Slabými stránkami naopak jsou krátká doba působení (méně než 5 let), vysoká zadluženost a minimální technický výhled do budoucnosti.

2.1.4.3 Příležitosti

Příležitosti jsou příznivé sociologické a ekonomické vnější faktory, také zde jsou možnosti, jak oproti konkurenci získat výrazný náskok v technickém zabezpečení.

2.1.4.4 Hrozby

Konkurence je nejsilnější hrozbou pro brněnskou ScioŠkolu, dalším rizikem je pomalá inovace nebo poškození pověsti neúspěchy absolventů při navazujícím studiu (SŠ, VŠ).

2.2 Informační systém Edookit

Edookit je školní informační systém vyvíjený společností EDOOKIT s.r.o. jejímž vlastníkem je od 19. února 2020 firma Unicorn Systems a.s. (14)

Systém provozuje firma pro všechny školy v cloudu a ty nemusí mít pro jeho funkčnost vlastní server, o vše se stará EDOOKIT s.r.o. Edookit obsahuje elektronickou třídní i žákovskou knihu, online matriku, administrativu školy, umožňuje také tvorbu rozvrhů, komunikaci v rámci školy a tiskové výstupy do pdf. (22)

Součástí platby za systém je jeho provoz, veškeré aktualizace, diskový prostor o velikosti 100 GB s možností zpoplatněného navýšení, pravidelné zálohování (4x denně) a nonstop technická podpora. Je možnost si připlatit za nadstandartní školení nebo prioritizaci vývoje nové funkce. Cena za systém pro školy do 200 žáků (ostatní uživatelé nejsou omezeni) je 26 300 Kč/rok. (22)

V současné době probíhá postupná migrace účtů informačního systému Edookit do IS Plus4U, aby bylo umožněno jednotné přihlášení v rámci celé společnosti.

2.2.1 EDOOKIT s.r.o.

Společnost Edookit s.r.o. byla zapsána do obchodního rejstříku v květnu 2009. Firma vznikla v Brně, kde měla sídlo až do 8. září 2020, tehdy se sídlo přesunulo do Prahy na stejnou adresu jako její vlastník společnost Unicorn Systems a.s. (14)

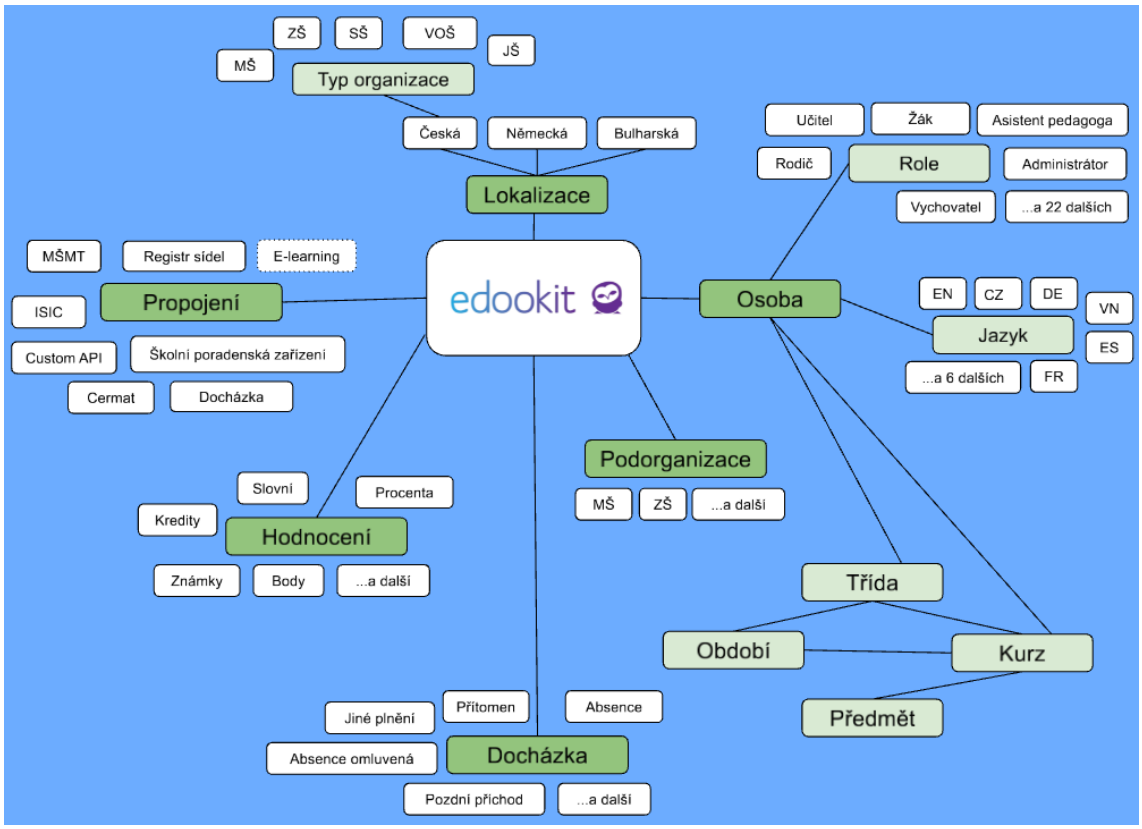
Hlavním produktem firmy je školní informační systém Edookit, který již využívají stovky škol v Česku. Edookit je cloudový systém, fyzicky systém běží ve dvou datových centrech v Evropské unii a data jsou několikrát denně zálohována. (22)

IS vznikl s vizí vytvořit moderní integrovanou platformu pro školy propojením administrativy a výukových nástrojů. Systém Edookit podporuje individualizaci výuky, e-learning a zapojení rodičů do výuky. Školám je systém poskytován společně se zákaznickou podporou, která řeší možné problémy a v návaznosti na zpětnou vazbu je software vyvíjen. Společnost pravidelně pořádá školení pro školy, ať už pro vyučující nebo pro administrátory systému. (22)

2.2.2 Informace od manažera firmy Edookit

Informační systém Edookit byl vytvořený na zelené louce jako nejnovější ze školních informačních systémů používaných v České republice. Od počátku byl vyvíjen jako čistě cloudový systém, aby se vyhnul náročné, nákladné a nedokonalé transformaci z lokálního systému na cloudový. Tato snaha se například IS Bakaláři vůbec nepovedla a jedná se o „pseudocloud“, který je řešen přes přístup na vzdálenou plochu. (23)

Edookit se zaměřuje na školu jako na proces a cílem je školní procesy správně navázat, aby logicky spolupracovali. Spolu s tím se soustředí na přehledné uživatelské rozhraní, které přesto umožňuje spravovat vše potřebné. Příkladem je možnost odlišné volby jazyka, ve kterém systém je zobrazen, pro uživatele od výchozího řešení školy. Dalším příkladem je provázanost suplování s rozvrhem a výkazem odučených hodin, kdy při tvorbě suplování si lze vyfiltrovat, kterému vyučujícímu chybí odučit hodiny a současně má v potřebné termíny volno a aprobaci na daný předmět. (23)



Obrázek 10 Principy Edookit (23)

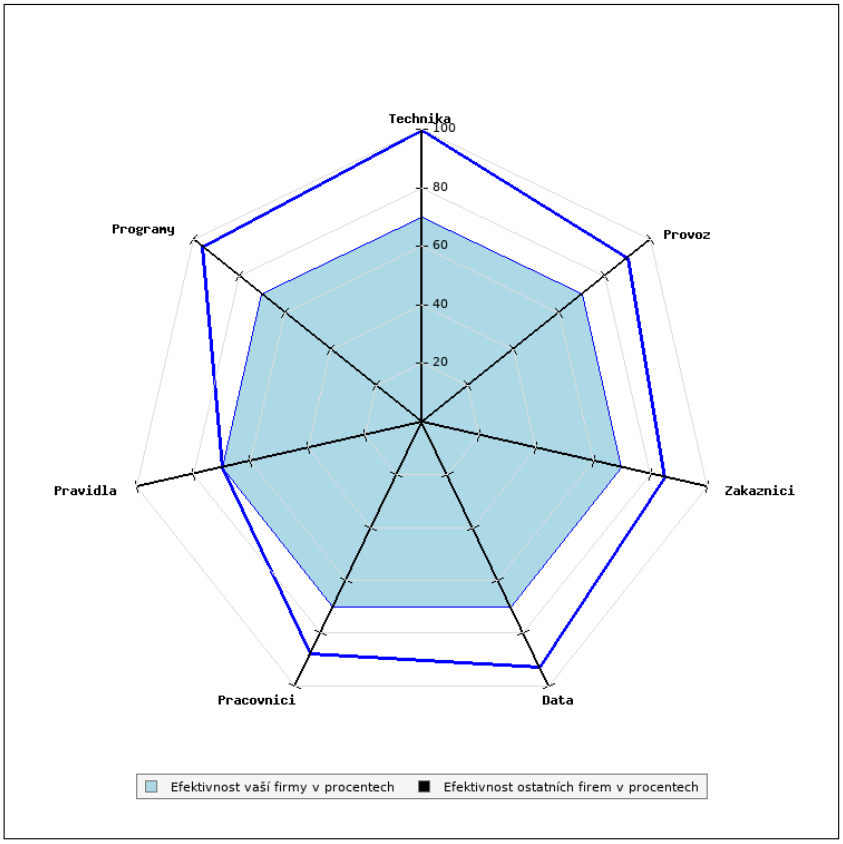
Edookit má za cíl směřovat i na zahraniční trhy, proto je možné při tvorbě školy definovat, pro který školní systém bude určen. V Česku se jedná o rozpětí od Mateřských škol (MŠ) po Vyšší odborné školy (VOŠ). (23)

Informační systém se od konkurenčních systémů odlišuje také jinou vazbou mezi žákem a rodičem. U jiných systémů je na jeden žákovský účet navázán právě jeden rodičovský účet a tento rodičovský účet je vždy propojen s právě jedním žákovským účtem, jedná se o vazbu 1:1. V Edookitu je běžné mít připojeny dva rodičovské účty a tyto rodičovské účty mohou být propojeny s více žákovskými účty (rodiče mívají i více dětí na stejné škole). (23)

Díky propojení s účty Plus4U bude například možné škole, jako celku nebo i jen po ročnících, nabídnout kurzy od Red Monster, po jejichž splnění se výsledek propíše do žákovského účtu v Edookitu. Problémem tohoto propojení je, že jedinečný identifikátor v Plus4U je e-mailová adresa uživatele a obzvláště mladší děti žádnou takovou adresu nemají. Tento nedostatek je aktuálně ve fázi řešení, aby mohla být migrace účtů úspěšně dokončena. (23)

2.3 Zefis analýza ScioŠkola Brno a IS Edookit

V analýze přes portál Zefis byl hodnocen IS Edookit a proces komunikace s rodiči, který je v dnešní době ještě důležitější než v „předcovidové“ době.



Obrázek 11 Graf analýzy efektivnosti (11)

Oblast	Moje firma
Technika	100%
Programy	96%
Pravidla	70%
Pracovníci	88%
Data	93%
Zákazníci	85%
Provoz	90%
Celkem	**70%**

Obrázek 12 Tabulka analýzy efektivnosti (11)

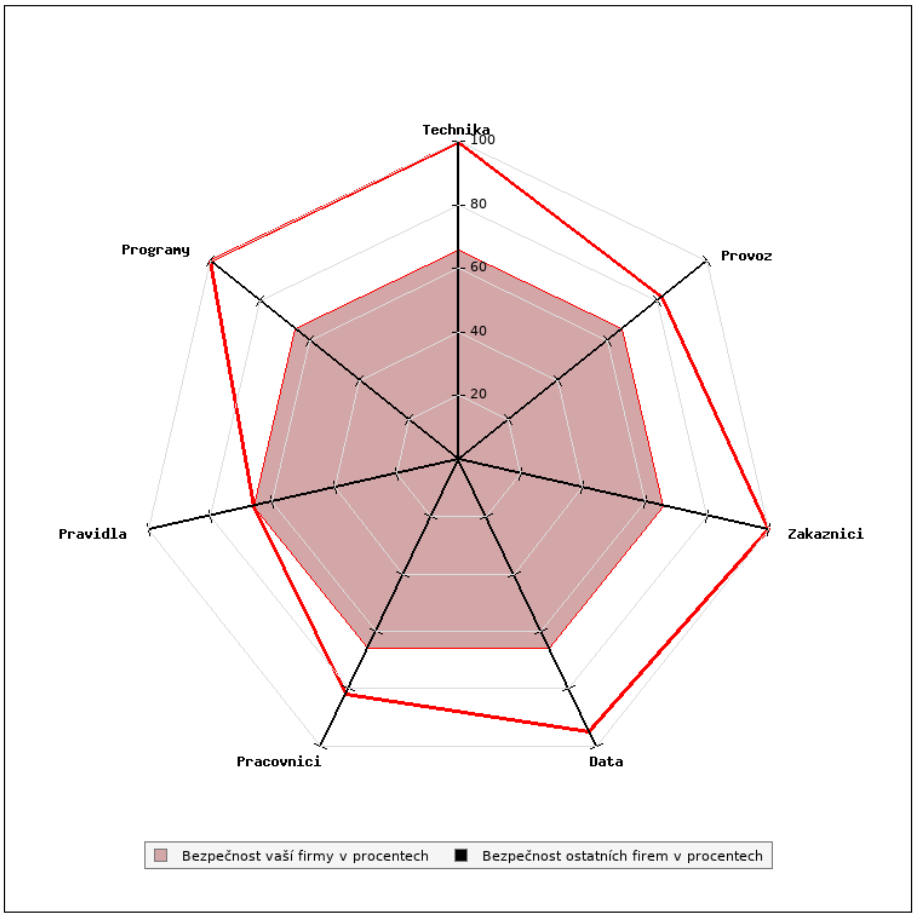
Největším problémem společnosti je oblast pravidel. O tomto nedostatku firma ví a snaží se jej řešit. Protože jde o školu, tak tvorba firemních politik pro informační bezpečnost není prioritou a vystačí si s průběžným školením zaměstnanců v této oblasti. Rozhodně se ale nejedná o dlouhodobě udržitelné řešení.

Oblast	Významnost	Bezpečnost	Typ	Název
Pravidla	Střední	Ne	Neshoda	Chybí manažer informačních systémů
Pravidla	Střední	Ne	Neshoda	Chybí informační strategie
Zákazníci	Střední	Ne	Neshoda	Nejsou propojeny systémy s daty pro zákazníky
Provoz	Střední	Ne	Neshoda	Pomalá doba odezvy technické podpory
Data	Nízká	Ne	Neshoda	Chybí pravidla pro zavedení dat do systému
Zákazníci	Nízká	Ne	Neshoda	Není zjišťováno, co zákazníci od informačního systému očekávají
Zákazníci	Nízká	Ne	Neshoda	Ignorování přání zákazníků
Zákazníci	Nízká	Ne	Neshoda	Nevhodný design systému pro zákazníky
Provoz	Nízká	Ne	Neshoda	Dlouhá doba vyřízení méně významného požadavku na podporu
Programy	Nízká	Ne	Neshoda	Špatné ovládání programu

Obrázek 13 Nedostatky v efektivnosti IS (11)

Problémy ve vztahu k zákazníkům jsou způsobeny tím, že zákazníky jsou rodiče žáků a případným řešitelem jejich problému je dodavatel IS, který nemůže vyhovět každému požadavku od všech uživatelů svého IS (nejen této školy). IS je ale pravidelně aktualizován a probíhají i změny podle potřeb zákazníků (škol a rodičů).

Zajímavé je doporučení s názvem „Zvážit nutnost přístupu na internet“, které je možné u mnoha jiných firem, ale v moderním školství je zcela nereálné. Je totiž běžné, aby studenti používali internetový vyhledávač, ověřovali si informace a přicházeli i se zajímavostmi na které narazili. Filtr nevhodného obsahu je realizován na úrovni DNS.



Obrázek 14 Graf analýzy bezpečnosti (11)

Oblast	Moje firma
Technika	100%
Programy	100%
Pravidla	66%
Pracovníci	82%
Data	95%
Zákazníci	100%
Provoz	82%
Celkem	**66%**

Obrázek 15 Tabulka analýzy bezpečnosti (11)

Také v oblasti bezpečnosti IS má nejnižší hodnocení oblast pravidel. Jedná se o stejné problémy jako v hodnocení efektivity IS, není zpracovaná informační strategie, bezpečnostní pravidla pro IS/ICT nejsou sepsána, jsou předávána pouze slovně a téměř nejsou vymáhána.

Oblast	Významnost	Bezpečnost	Typ	Název
Pravidla	Vysoká	Ano	Neshoda	Chybějící, nebo špatně dodržovaná bezpečnostní pravidla
Provoz	Vysoká	Ano	Neshoda	Bezpečnostní hrozba virového útoku
Pravidla	Vysoká	Ano	Neshoda	Chybí klasifikace dat/ informací
Pravidla	Vysoká	Ano	Neshoda	Chybí bezpečnostní pravidla informačního systému
Pracovníci	Vysoká	Ano	Neshoda	Nejsou aktualizovaná hesla uživatelů
Pravidla	Střední	Ano	Neshoda	Chybí strategie bezpečnosti
Pravidla	Střední	Ano	Neshoda	Chybí manažer/ka informační bezpečnosti
Pracovníci	Střední	Ano	Neshoda	Přístupová práva zaměstnanců nejsou včas nastavována
Pracovníci	Střední	Ano	Neshoda	Bezpečnostní hrozba z přístupu na internet
Data	Střední	Ano	Neshoda	Riziko zneužití dat, virového útoku
Pravidla	Nízká	Ano	Neshoda	Špatně nastavené pracovní postupy
Pravidla	Nízká	Ano	Neshoda	Chybí pracovní postupy a pravidla pro práci s informačním systémem
Pracovníci	Nízká	Ano	Neshoda	Není vytvářeno bezpečnostní povědomí pracovníků
Pracovníci	Nízká	Ano	Neshoda	Neprobíhají periodická bezpečnostní školení uživatelů IS

Obrázek 16 Nedostatky v bezpečnosti IS (11)

Vysokou významnost u hrozby virového útoku lze označit za běžný jev v celém IT světě. V případě ScioŠkoly lze pouze konstatovat, že pokud by tato situace nastala, tak IS je ve správě společnosti Edookit s.r.o. a data zde jsou pravidelně zálohována a bez pracovních stanic by ve ScioŠkole šlo krátkodobě fungovat. Data jsou opět pravidelně zálohována do cloudu a současně na offline uložiště.

Problémy v oblasti pracovníků jsou propojeny s nedostatky v pravidlech a v jejich striktním nevymáhání. Upozornění na neaktualizovaná hesla je způsobeno prevencí v psaní si hesel na papír. Raději ať pracovníci používají 2 roky stejné heslo, když si ho budou pamatovat, než každé 3 měsíce vyžadovat jeho změnu a zvýšené riziko „papírku na monitoru“.

2.4 Hardware

Ve škole se nachází řada různých zařízení. Převažují notebooky, které jsou od několika značek – Lenovo, HP, Asus. Přibližně polovina je určena pro zaměstnance školy a zbylá polovina pro žáky během výuky. V době distanční výuky byly (jsou) některé studentské notebooky půjčeny žákům pro vzdálené vzdělávání. V několika třídách jsou také interaktivní tabule s projektory, další projektory jsou přenosné pro případ jeho potřeby ve třídě bez tohoto vybavení. Hlavně mladší žáci si půjčují také školní tablety místo notebooků. Celá budovy školy je pokryta wifi signálem z několika zařízení Ubiquiti UniFi AC PRO.

2.5 Software

Na většině zařízeních je jako operační systém nainstalován Windows 10 Pro, v několika je systém Windows 10 Home. Na pár zařízeních je také linuxový operační systém Fedora 32 a na tabletech se nachází systém Android. Postupně je snaha opustit systém Windows 10 Home a dokončit přechod na Windows 10 Pro.

Z hlediska programového vybavení je na všech počítačích stejná skladba programů, aby se žáci ani učitelé dokázali vždy okamžitě zorientovat. Jedná se o následující programy: nejmenovaný antivir, kancelářský balík LibreOffice, webové prohlížeče Google Chrome, Mozzila Firefox a Edge, multimediální přehrávač VLC media player, prohlížeč pdf formátu Adobe Acrobat Reader, 7-Zip pro práci s komprimovanými soubory, základní údržba operačního systému pomocí Ccleaner, programy pro práci s grafikou Gimp, Inkscape a Krita a herní engine Unity.

Na noteboocích s Fedorou se nenachází programy Edge a Unity a Google Chrome je nahrazen linuxovou verzí, která se nazývá Chromium. Programová výbava na tabletech je zaměřena na různé vzdělávací aplikace z Google Play (například Tablexia, Duolingo a mnoho dalších), antivir a aplikace, které jsou dodávány s operačním systémem.

2.6 Rozhovory s uživateli IS

Ohledně Edookitu uživatelé kladně hodnotí zpracování třídní knihy, docházky a snadné dohledání kontaktních údajů jednotlivých žáků a jejich rodičů. Dále si chválí, že hned na úvodní obrazovce je zobrazený rozvrh uživatele a pro vyučující je snadné do něj vkládat

docházku a učivo (vést třídní knihu). Dobrou vlastností je také možnost změnit odeslanou zprávu, například kvůli opravení chyby.

Jako nevýhody systému uživatelé uvádí časově náročné změny ve složení studijních skupin nebo v administraci jednotlivých uživatelů. Edookit se prezentuje jako jednotné řešení pro celou školu, bez potřeby dalších IS, ale spravovat zde například školní knihovnu nebo jej používat k distanční výuce není vhodné a jiná řešení jsou uživatelsky přívětivější. V případě odesílání zpráv chybí možnost šablon a použití skryté kopie. Někteří uživatelé by ocenili, aby zprávy fungovaly jako e-maily. Problémem je také odlišný formát papíru pro vysvědčení 9. tříd, které má sloužit jako doklad o ukončeném studiu, ale IS Edookit tuto volbu při tisku vysvědčení nemá a je potřeba manuálně měnit oblast tisku.

Vyučující, kteří mají zkušenosti i s jiným školním systémem, tak IS Edookit hodnotí jako výrazně lepší volbu.

Zaměstnanci si chválí v provozu IT ochotu řešit problémy a ve většině případů jejich úspěšné vyřešení, oceňují oddělení wifi sítě pro zaměstnance, žáky a veřejnost, kdy každá ze sítí má odlišné nastavení. Za výhodu označují postupný rozvoj školy v IT oblasti, která tak nestagnuje.

Nevýhodou pro školní IT je v mnoha případech nemožnost řešit problém v okamžiku vzniku, protože se technik nenachází v prostorách školy a mezi vznikem a řešením triviálního problému může být prodleva i v řádu několika dnů. I přes postupný rozvoj by vyučující ocenili tento rozvoj urychlit a mít jasně definované priority a dobu řešení.

2.7 Souhrn analýz

Společnost ScioŠkola Brno je mladá společnost, která ale již pár let vykazuje kladný výsledek hospodaření a postupně splácí dluh vůči zřizovateli vzniklý při zakládání firmy. Dokázala tedy za krátký čas vyplnit mezeru na trhu a získat si dostatečné množství zákazníků, aby hospodařila v černých číslech.

Škola je zaměřená na vzdělávání a ostatní oblasti podnikání jsou na vedlejší koleji, například IT strategie není ve škole jedno z podstatných témat.

Také je potřeba si nadále držet zákazníky, jejich odchod je největším rizikem možného úpadku školy. Není možné si je zavázat na několik let a je potřeba je neustále přesvědčovat o správném výběru vzdělání právě na ScioŠkole pro jejich dítě/děti.

Kromě potřeby zákazníků je důležité mít zaměstnance, kteří budou sdílet stejné hodnoty a budou je umět předat i žákům, bez těchto zaměstnanců by totiž ScioŠkola nebyla odlišná od své konkurence.

Informační systém Edookit je dobrou volbou pro ScioŠkolu, protože nabízí všechny nutné funkce v přehledném rozhraní a nejsou s ním žádné výrazné problémy. Zároveň je ze strany provozovatele výrazná snaha neustále Edookit vyvíjet i na základě podnětů od jeho uživatelů.

Pro školu je nevýhodná nepředvídatelnost základních IT služeb, které nejsou poskytovány externí společností, přesto není zájem si tímto způsobem službu od jiného dodavatele zakoupit, kvůli negativním zkušenostem z jiných škol. Je tedy potřeba zpracovat IT strategii, aby bylo jasně definováno, kterým směrem se bude investovat do IT a také mít přesně určené nejen bezpečnostní politiky.

3 VLASTNÍ NÁVRHY ŘEŠENÍ

Poslední částí diplomové práce se zabývá návrhem řešení. Tento návrh reaguje na nedostatky nalezené v analytické části. Změna bude nejprve vyjádřena slovním popisem, na který naváže zpracování pomocí Lewinova modelu. Další částí bude analýza rizik, která mohou mít dopad při provádění změny. Na zpracování návrhů opatření vycházejících z analýzy rizik navazuje časová analýza PERT, pomocí níž se zjistí časová náročnost projektu. Poslední částí je ekonomické zhodnocení včetně návrhu rozpočtu.

3.1 Popis návrhů změn

Je potřeba vypracovat soubor firemních politik a strategií. Podle tohoto dokumentu poté musí probíhat kontrola jejich dodržování. Samotný proces kontroly musí být zahrnutý v dokumentu obsahujícím bezpečnostní pravidla, která budou kontrolována.

Konkrétně se jedná o dokument obsahující firemní informační strategie. V tomto souboru je nutné definovat osobu odpovědnou za informační aktiva, za jakých podmínek se nutné dokoupit nové IT zařízení a jaké parametry tyto zařízení musí splňovat. Další částí budou školení uživatelů v IT oblasti. V závěru dokument představí výhled do budoucnosti, kam by v oblasti IT se dalo investovat pro usnadnění chodu školy.

V bezpečnostní strategii bude zahrnuta heslová politika společnosti, bezpečnostní pravidla pro uživatele, způsob likvidace IT zařízeních po skončení jejich životnosti a bezpečnostní školení pro všechny uživatele.

Poslední navrhovanou změnou je účast na školeních pro ovládání IS, které pravidelně pořádá dodavatel školního informačního systému Edookit.

3.2 Lewinův model

Jedná se o model změny, který se skládá ze tří fází – rozmrazení, přechodu a aplikace změny a zmrazení.

3.2.1 Fáze rozmrazení

V následující tabulce se nachází analýza silového pole. Jedná se o analýzu, která určí, jestli navrhovaná změna je pro firmu prospěšná. Ve sloupci Síla je slovně popsána síla,

která má vliv na zavedení změny. Ve sloupci Hodnota jsou hodnoty od -10 do +10, kdy záporná čísla jsou proti změně a kladná pro změnu. V posledním řádku je suma všech hodnot a pokud tento součet vyjde kladný jedná se o prospěšnou změnu, v případě záporného výsledku není změna vhodná, protože převažují negativa nad přínosy. Pokud hodnota vyjde nula, tak změna nemá ani pozitivní ani negativní výsledek.

Tabulka 1 Analýza silového pole (vlastní zpracování)

Síla	**Hodnota**
Usnadnění práce IT konzultanta	+8
Ušetření času, díky definované odpovědnosti	+2
Zvýšení IT bezpečnosti	+10
Podpora od vedení společnosti	+2
Podpora změny od některých zaměstnanců	+6
Časová náročnost zavedení změny	-6
Finanční náročnost zavedení změny	-4
Nesouhlas některých zaměstnanců se změnou	-3
Celkem	**+15**

Výsledná hodnota vyšla kladná, změna by tedy měla být pro společnost prospěšná.

Agentem změny je IT konzultant, který již nyní má IT ve společnosti na starost a je iniciátorem této změny. Sponzorem změny je ředitel školy, který změnu hradí z rozpočtu a vyčlení i čas ostatních zaměstnanců pro navazující pravidelná školení. Advokáti změny jsou někteří zaměstnanci, kteří chodili s dílčími problémy a které by vypracování strategie a pravidelná školení vyřešilo s předstihem.

Jedná se převážně o změnu interních procesů firmy. Lidské zdroje a jejich řízení ani organizační struktura tedy nebudou nijak zasaženy touto změnou. Technologie firmy mohou být změnou zasaženy v dlouhodobém měřítku, když se díky pravidelným kontrolám dojde k závěru, že je třeba přepracovat používané informační systémy. Firemní procesy v oblasti IT budou lépe definovány a měly by se minimalizovat situace, kdy si uživatelé nejsou jistí, na koho se v případě problému obrátit.

3.2.2 Fáze změny

Jedná se o provedení následujících činností.

Tabulka 2 Seznam činností (vlastní zpracování)

Označení činnosti	Popis činnosti
A	Analýza současného stavu
B	Zjištění požadavků zaměstnanců
C	Schválení nutnosti změn vedením
D	Vypracování politik pro IT bezpečnost
E	Vypracování IT strategie
F	Schválení dokumentů vedením
G	Dokoupení potřebné techniky
H	Uvedení této techniky do provozu
I	Příprava školení IT
J	Příprava školení IT bezpečnost
K	Školení IT
L	Školení IT bezpečnost
M	Zjištění zpětné vazby od uživatelů
N	Reakce na zpětnou vazbu
O	Úprava pravidel v IT bezpečnosti
P	Úprava IT strategie
Q	Schválení opravených dokumentů
R	Kontrola dodržování IT politik

Činnosti A a B jsou součástí této práce v analytické části.

Při jakémkoliv schvalování je potřeba vzít do úvahy důvody zamítnutí a případně je zahrnout do opravené verze žádosti o schválení.

Vypracování politik pro IT bezpečnost zahrnuje definování heslové politiky, pravidelnost a obsah bezpečnostních školení, bezpečnostní nastavení všech IT zařízení (například počítačů, mobilních telefonů nebo síťových prvků), analýza rizik, seznam možných hrozeb a jejich řešení, pokud by nastaly.

Při vypracování IT strategie je nutné sepsat podmínky, které musí splňovat jednotlivá koncová zařízení (počítače, notebooky, tablety, mobily…), jaký je optimální počet těchto zařízení, seznam potřebných programů těchto zařízení (dle jejich předpokládaného využití), definování pravidel pro práci IT konzultanta, soupis znalostí, které by měli znát všichni uživatelé školních IT zařízení a pravidelnost školení k těmto znalostem, návrh cíle, které ho se chce dosáhnout v následujícím období (může se jednat o rok nebo i 5 let).

Činnost G zahrnuje techniku, která je označena jako potřebná vypracováním IT strategie. Její uvedení do provozu, zahrnuje nastavení těchto zařízení podle pravidel v IT strategii a IT bezpečnosti.

Příprava školení znamená nachystaní si osnovy (prezentace), podle které školení bude postupovat. Na samotné školení přímo navazuje zpětná vazba od účastníků. Úprava dokumentace je vhodná na základě této zpětné vazby, například se může jednat o podcenění znalostí uživatelů nebo naopak o jejich přecenění. Tuto úpravu je opět nutné schválit vedením společnosti.

Posledním krokem je kontrola dodržování nastavených politik, zda uživatelé tyto nastavená pravidla dodržují.

Následuje podrobnější popis některých činností, respektive jejich částí.

3.2.2.1 Vypracování politik pro IT bezpečnost

Heslová politika, znamená definování minimální délky hesel, podmínky pro jejich tvorbu – například aby heslo obsahovalo alespoň jedno číslo, malé a velké písmeno a nějaký speciální znak jako je tečka, čárka, vykřičník…, doba, po které je nutné hesla změnit. Nejedná se pouze o podmínky pro běžné uživatele, ale i pro IT konzultanta, který mimo zařízení pro ostatní uživatele spravuje i síťové prvky.

Bezpečnostní školení by měla obsahovat nejčastější hrozby, které se v IT světě objevují a jak se jim vyhnout. Dále by jejich součástí měla být seznámení uživatelů se základními bezpečnostními návyky, například nestahovat každou přílohu v mailu, být podezřívavý, ověřovat https certifikát, nepoužívat stejné heslo pro všechny služby atd.

3.2.2.2 Vypracování IT strategie

U podmínek pro nová koncová zařízení se jedná o minimální výpočetní výkon, kapacitu disku nebo paměti. Počet těchto zařízení by se měl odvíjet od počtu zaměstnanců nebo žáků (podle jejich určení, například počet učitelských zařízení nezáleží na počtu žáků).

Důležitou částí je také jasné definování SLA pro IT konzultanta, který má na starosti správu IT zařízení, která jsou ve škole používána, ale který není zaměstnancem na plný úvazek a ve společnosti pracuje pouze na dohodu o provedení práce. IT konzultant by měl mít jednoznačně definované podmínky, jak rychle je nutné řešit závady dle potřebné priority.

Součástí také musí být vytvoření pravidel pro likvidaci IT zařízení při konci jejich životnosti.

Výhled do budoucna by měl obsahovat odhadovaný stav IT za zvolený počet let. Jednak v ohledem na rozvoj nových technologií, také podle předpokládaného vývoje velikosti školy. Může se jednat o integraci nových IS, přechod na lepší WiFi standard nebo například o stavební úpravy, které budou vyžadovat změny v IT.

3.2.2.3 Školení

Součástí školení by mělo být zjištění na jaké úrovni jsou znalosti účastníků a podle toho se snažit pojmout samotné školení. Také se musí jednat o interaktivní školení, jinak z něj účastníci velice rychle zapomínají, o čem školení bylo a nic si z něj neodnesou.

Je potřeba odlišit školení, která budou pro zaměstnance školy a pro její žáky.

V případě žáků je potřeba rozhodnout, kdo bude žáky školit, jestli to bude IT konzultant nebo spíš proškolený průvodce, který na rozdíl od IT konzultanta má pedagogické vzdělání. Školení pro žáky by bylo potřeba zahrnout do běžné výuky, pravděpodobně jako součást informatiky (v rámci předmětu Svět v souvislostech). IT konzultant by mohl být součástí této výuky a na přípravě hodiny by se podílel spolu s průvodcem.

Základní školení zaměstnanců by se mělo odehrávat v době jejich nástupu a pravidelná jednou za rok, přičemž vhodným termínem by mohl být konec letních prázdnin, před začátkem výuky.

Zpětná vazba na školení se očekává od obou skupin účastníků, ale v případě žáků je potřeba k ní přistoupit odlišně než ke zpětné vazbě od dospělých zaměstnanců.

Školení na informační systém Edookit nabízí přímo poskytovatel tohoto systému v pravidelných intervalech. Základní školení pro učitele má dokonce zveřejněné v podobě video záznamu na svých stránkách https://edookit.com/cs/training-teachers. Různá další školení pro učitele nebo administrátory systému pořádá online formou půldenního webináře, který je zpoplatněn 1 500 Kč za účastníka.

3.2.2.4 Kontrola dodržování IT politik

Je nutné stanovit odpovědnou osobu za tuto kontrolu. Mělo by se jednat o IT konzultanta, protože tyto politiky zná nejlépe a má na starost i jejich školení.

Obtížnější je stanovit, jak tyto politiky kontrolovat. ScioŠkola si zakládá na důvěře mezi zaměstnanci a není žádoucí, aby zaměstnancům byl pravidelně kontrolován pracovní notebook, zda dodržují všechny IT politiky. Zaměstnanci ale mají možnost si tuto kontrolu nechat provést na požádání. Může se jednat o případ, kdy mají podezření na možný bezpečnostní incident nebo jen mohou potřebovat poradit, zda jimi zvolený program je vhodný k instalaci na školní zařízení. Další možnou kontrolou může být občasný test v podobě emailové phishingu, který ale bude muset být předem domluvený s IT týmem v Praze. Ten má na starost správu domény scioskola.cz, aby nenastala z jejich strany obava o možný skutečný útok na ScioŠkolu.

V případě zařízení dostupných pro žáky školy je situace jednodušší. Tyto zařízení jsou pravidelně kontrolována, jsou zde promazávány různé dočasné soubory (cookies webových prohlížečů, prohlížečová mezipaměť, uložená hesla a další).

3.2.3 Fáze zmrazení

Zjištění úspěšnosti provedení změn. Lze zjistit pomocí opětovné zpětné vazby od uživatelů v době po zavedení změn. Druhou možností pro zjištění úspěšnosti je během kontrol dodržování nově zavedených pravidel. Pokud by nebyla dodržována, tak se jedná buď o neúspěšná školení nebo o chyby ve vypracované strategii. V těchto případech je potřeba reagovat úpravou IT strategie nebo vylepšením školení (častější, atraktivnější, snáze pochopitelné a více vysvětlující, proč jsou tato pravidla nutná).

Příkladem možných chyb ve strategii může být absence možného případu využití zařízení a s tím spojená absence programu, který tuto funkci dodá.

3.3 Analýza rizik

V analýze rizik je použita skórovací metoda. Vysvětlující tabulka pro pravděpodobnost vzniku rizika a jeho dopadu je zobrazena níže.

Tabulka 3 Skórovací metoda (vlastní zpracování)

Hodnota pravděpodobnosti	**Pravděpodobnost v %**	**Hodnota dopadu**	**Dopad na projekt**
1–2	0–20	1–2	Minimální
3–4	21–40	3–4	Nízký
5–6	41–60	5–6	Střední
7–8	61–80	7–8	Vysoký
9–10	81–100	9–10	Kritický

Následující tabulka obsahuje seznam deseti hrozeb a jejich možných scénářů spolu s hodnotami pravděpodobnosti výskytu (sloupec P) a hodnotami dopadu na projekt (sloupec D), výsledná hodnota rizika je vypočtena vynásobením předchozích hodnot a nachází se ve sloupci R.

Rovnice 2 Výpočet hodnoty rizika (vlastní zpracování)

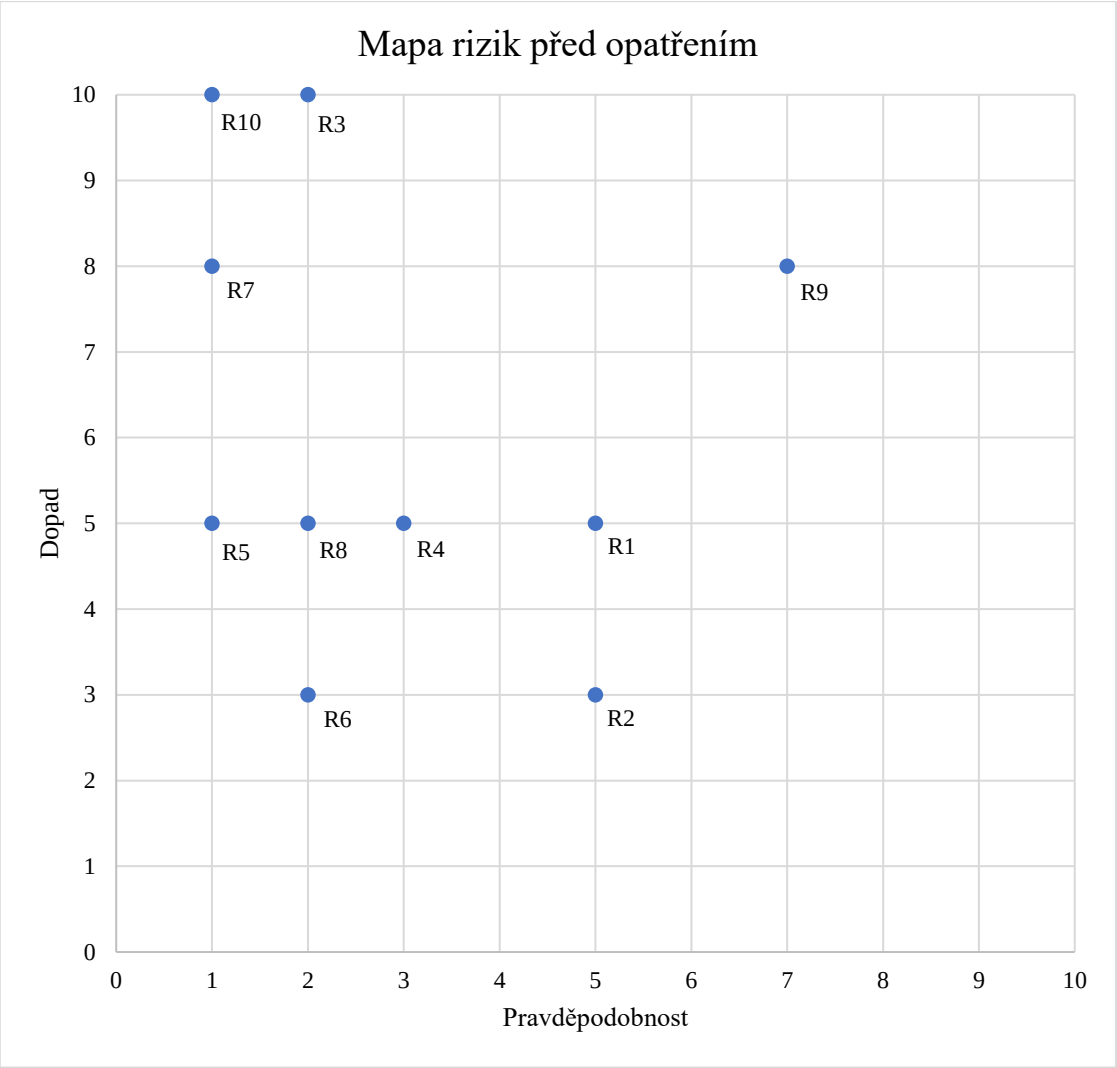
Nejedná se o konečný seznam možných hrozeb, pouze několik možných příkladů. Celkem se může jednat o stovky hrozeb, které mohou nastat, v případě větší společnosti i o tisíce.

Tabulka 4 Analýza rizik (vlastní zpracování)

ID	**Hrozba**	**Scénář**	**P**	**D**	**R**
R1	Špatný návrh rozpočtu	Nebude dost finančních prostředků pro provedení změny	5	5	**25**
R2	Špatná časová analýza	Změna se nestihne provést v požadovaném termínu	5	3	**15**
R3	Sponzorovi změny se dokument nebude zamlouvat	Odmítnutí zavedení změny vedením	2	10	**20**

R4	Špatné školení uživatelů	Uživatelé nebudou novým pravidlům rozumět	3	5	**15**
R5	Nesouhlas uživatelů s novými pravidly	Uživatelé pravidla úmyslně nedodržují	1	5	**5**
R6	Špatný nákup nové techniky	Nová technika nefunguje podle očekávání	2	3	**6**
R7	Špatný analýza současného stavu	Nepřesné určení, co je potřeba	1	8	**8**
R8	Nedostatek prostoru pro pravidelné kontroly	Uživatelé nedodržují pravidla	2	5	**10**
R9	Nedokončení celé změny	Agent změny opustí pracovní pozici	7	8	**56**
R10	Změna názoru vedení na dokument po zavedení	Průběžná údržba bude příliš nákladná	1	10	**10**

Mapa rizik graficky zobrazující výsledky z předchozí tabulky. Z grafu je poznat, že největší hrozbou je R9, která popisuje odchod agenta změny z pracovní pozice ve firmě.



Graf 1 Mapa rizik před opatřením (vlastní zpracování)

Tabulka s riziky, kde jsou již zahrnuty návrhy opatření, která snižují pravděpodobnost výskytu rizika nebo jeho dopad na projekt změny.

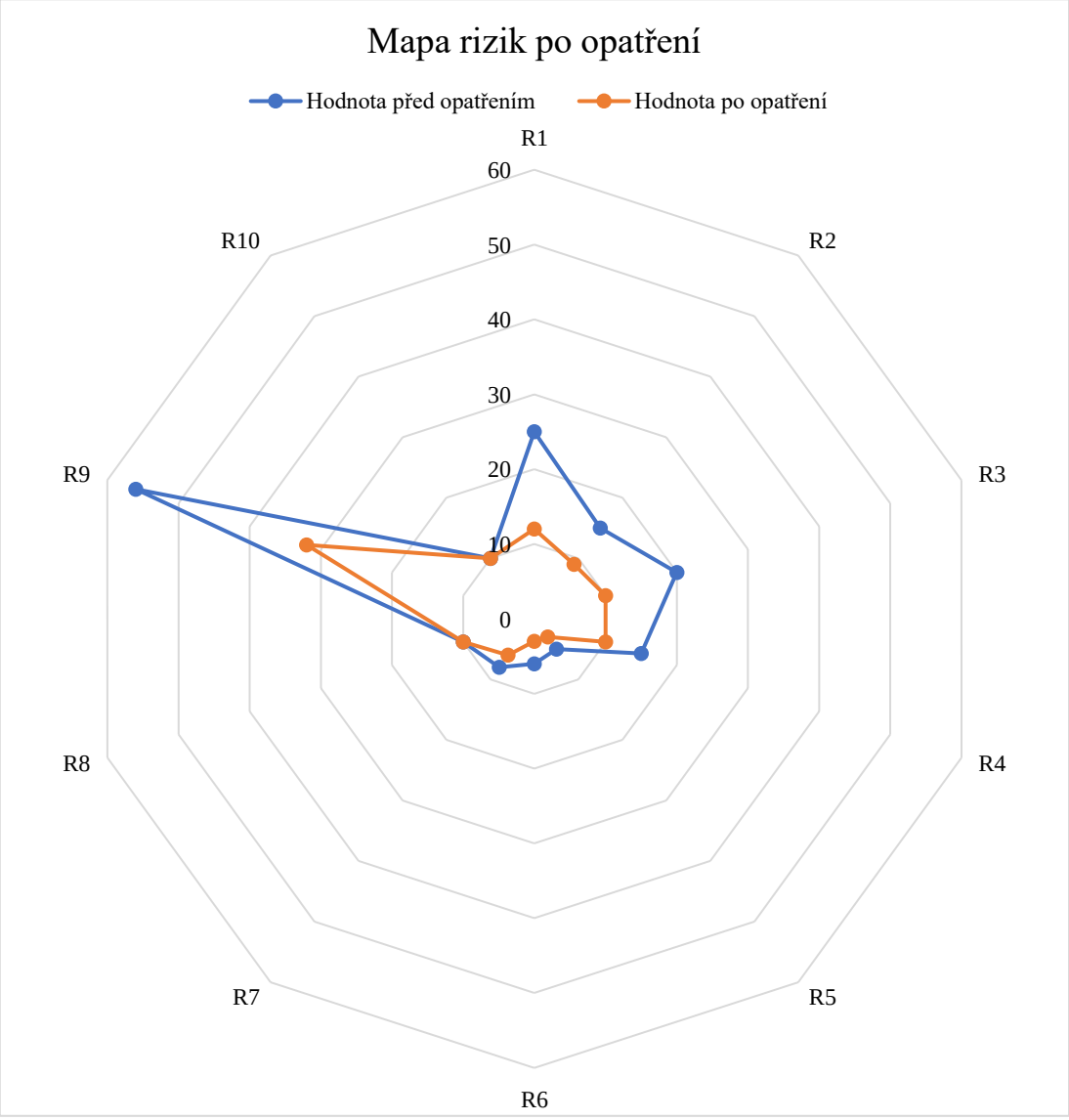
Tabulka 5 Návrh a vliv opatření (vlastní zpracování)

ID	Návrh opatření	P	D	R
R1	Finanční rezerva v rozpočtu	3	4	**12**
R2	Časová rezerva	3	3	**9**
R3	Průběžné konzultace o dokumentu	1	10	**10**
R4	Tvorba školení ve více lidech	2	5	**10**
R5	Lepší vysvětlení, proč je to potřeba	1	3	**3**

R6	Nákup u ověřeného prodejce/reklamace	1	3	**3**
R7	Konzultace s další kompetentní osobou	1	6	**6**
R8	Akceptace rizika	2	5	**10**
R9	Zlepšit motivaci klíčového zaměstnance	4	8	**32**
R10	Akceptace rizika	1	10	**10**

Riziko odchodu klíčového zaměstnance bylo sníženo zlepšením jeho motivace pro dokončení změny. Může se jednat o finanční hodnocení nebo o návrh na delší pracovní úvazek.

Poslední částí analýzy rizik je pavučinový graf porovnávající stav před a po zavedení opatření.



Graf 2 Pavučinový graf mapy rizik po opatřeních (vlastní zpracování)

Z grafu je snadno vidět, že většina hrozeb byla snížena pod hodnotu 15, kdy už lze hovořit o zanedbatelném výsledku. Nebezpečím stále zůstává R9, které ale není možné více snížit, protože by to bylo finančně nevýhodné. Bylo by poté lepším řešením předat rozdělanou práci novému IT konzultantovi, kterému to bude trvat déle, ale již bude nízká pravděpodobnost na nedokončení změny.

3.4 Časová analýza PERT

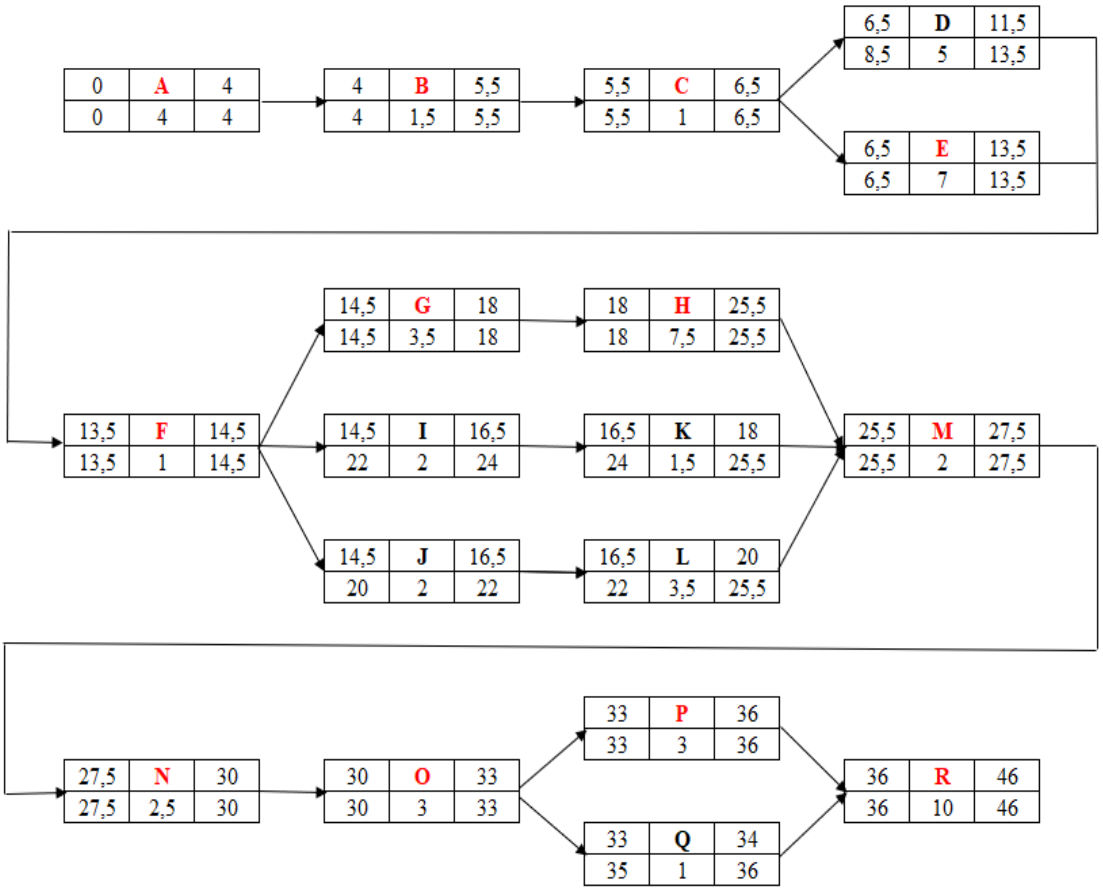
Následuje tabulka se seznamem činností, provázaností, délkou jejich trvání a časovou rezervou.

Tabulka 6 Časová analýza PERT (vlastní zpracování)

Údaje o postupnosti činností projektu				Trvání (dny)				Stat. uk.		Ter. zahájení a ukončení činností				Rezerva
Označení činnosti	**Popis činnosti**	**i**	**j**	**a**	**b**	**m**	**t(ij)**	**σ2**	**σ**	**ZM**	**KM**	**ZP**	**KP**	**RC**
A	Analýza současného stavu	-	B	3	5	4	**4**	0,11	0,33	0	4	0	4	**0**
B	Zjištění požadavků zaměstnanců	A	C	1	4	1	**1,5**	0,25	0,5	4	5,5	4	5,5	**0**
C	Schválení nutnosti změn vedením	B	D, E	1	1	1	**1**	0	0	5,5	6,5	5,5	6,5	**0**
D	Vypracování politik pro IT bezpečnost	C	F	3	7	5	**5**	0,44	0,67	6,5	11,5	8,5	13,5	**2**
E	Vypracování IT strategie	C	F	3	15	6	**7**	4	2	6,5	13,5	6,5	13,5	**0**
F	Schválení dokumentů vedením	D, E	G, I, J	1	1	1	**1**	0	0	13,5	14,5	13,5	14,5	**0**
G	Dokoupení potřebné techniky	F	H	2	7	3	**3,5**	0,69	0,83	14,5	18	14,5	18	**0**
H	Uvedení této techniky do provozu	G	M	5	12	7	**7,5**	1,36	1,17	18	25,5	18	25,5	**0**
I	Příprava školení IT	F	K	1	3	2	**2**	0,11	0,33	14,5	16,5	22	24	**7,5**
J	Příprava školení IT bezpečnost	F	L	1	3	2	**2**	0,11	0,33	14,5	16,5	20	22	**5,5**
K	Školení IT	I	M	1	4	1	**1,5**	0,25	0,5	16,5	18	24	25,5	**7,5**
L	Školení IT bezpečnost	J	M	1	8	3	**3,5**	1,36	1,17	16,5	20	22	25,5	**5,5**
M	Zjištění zpětné vazby od uživatelů	H, K, L	N	1	3	2	**2**	0,11	0,33	25,5	27,5	25,5	27,5	**0**
N	Reakce na zpětnou vazbu	M	O	1	6	2	**2,5**	0,69	0,83	27,5	30	27,5	30	**0**
O	Úprava pravidel v IT bezpečnosti	N	P, Q	2	4	3	**3**	0,11	0,33	30	33	30	33	**0**
P	Úprava IT strategie	O	R	2	4	3	**3**	0,11	0,33	33	36	33	36	**0**
Q	Schválení opravených dokumentů	O	R	1	1	1	**1**	0	0	33	34	35	36	**2**
R	Kontrola dodržování IT politik	P, Q	-	5	15	10	**10**	2,78	1,67	36	46	36	46	**0**

V tabulce jsou červeně označeny nulové rezervy, pro tyto činnosti platí, že pokud se zpozdí, tak se opozdí celý projekt.

Na tabulku dále navazuje síťový graf, kde je přehledněji vyznačena návaznost jednotlivých činností. Červeně jsou označeny činnosti, které leží na kritické cestě.



Obrázek 17 Síťový graf PERT (vlastní zpracování)

Celková doba trvání projektu je 46 pracovních dnů, což je 368 hodin. Tento údaj je potřebný v rozpočtu pro výpočet finanční náročnosti pracovníků, kteří se tomuto projektu budou věnovat.

Kritická cesta prochází přes činnosti A-B-C-E-F-G-H-M-N-O-P-R.

3.5 Ekonomické zhodnocení

Mimo školení ohledně informačního systému lze využít interní zdroje pro tyto změny. Školení pro práci v Edookitu by bylo vhodnější od poskytovatele IS, který tato školení nabízí pravidelně každý měsíc v ceně 1 500 Kč/osoba.

Pokud by se v průběhu roku těchto školení účastnilo celkem 5 osob, tak cenové náklady ve výši 7 500 Kč/rok jsou téměř zanedbatelné a přínos je rozhodně vyšší, protože se o nově nabyté vědomosti může podělit i s ostatními zaměstnanci společnosti.

V následujících tabulkách je zobrazen odhad rozpočtu pro zavedení změn.

Tabulka 7 Návrh rozpočtu během 1. roku (vlastní zpracování)

Položka	**Náklady (Kč)**
Mzdy	75 000
Technika	100 000
Školení IS	7 500
Celkem	182 500

Odhadovaná finanční náročnost na zavedení změn je 182 500 Kč.

Tabulka 8 Návrh rozpočtu pro následující roky (vlastní zpracování)

Položka	**Náklady (Kč)**
Mzdy	30 000
Technika	80 000
Školení IS	7 500
Celkem	117 500

Předpokládané roční náklady pro následující roky jsou 117 500 Kč.

Ve mzdách jsou zahrnuty náklady pouze na školení uživatelů a na jejich kontrolu, což jsou činnosti, které probíhají pravidelně a úpravy dokumentace zaberou výrazně kratší časové období než při jejich tvorbě.

Nižší rozpočet na techniku je z důvodu dokoupení nezbytné techniky již v prvním roce a není zde započtena možnost neočekávaného růstu počtu uživatelů. Jedná se o finance na průběžnou obnovu IT zařízení.

ZÁVĚR

Tato diplomová práce má za cíl analyzovat stav informačního systému společnosti ScioŠkola Brno – základní škola s.r.o. a navrhnout změny, které zlepší fungování tohoto systému v oblastech bezpečnosti a efektivnosti.

V teoretické části jsou vysvětleny základní pojmy a jsou představeny různé analýzy a metody, které jsou použity v navazujících kapitolách. Důležitou částí je seznámení se s různými typy informačních systémů a s pohledem na bezpečnost těchto systémů.

Analytická část se zabývá vnějším okolím a vnitřním uspořádáním analyzované společnosti. Pro analýzu vnějšího okolí je použitá analýza SLEPTE a Porterova analýza. K vnitřnímu rozboru firmy je použita analýza 7S. Tyto analýzy slouží jako vstupní údaje pro SWOT analýzu. Na analýzu firmy navazuje analýza informačního systému, pomocí informací od manažera společnosti Edookit (dodavatele IS) a díky Zefis analýze od pana docenta Kocha. Dále navazuje zpětná vazba od zaměstnanců ScioŠkoly Brno a shrnutí všech analýz.

Z analytické části vychází návrhová část, která obsahuje návrh několika změn. Jedná se o vypracování bezpečnostní strategie a IT strategie. Spolu s přesněji definovanými školeními uživatelů. Společně by měly dlouhodobě zvedat IT povědomí mezi firemními zaměstnanci. Součástí těchto návrhů je také analýza časové a finanční náročnosti, spolu s analýzou možných rizik, aby se předešlo nedokončení těchto změn.

BIBLIOGRAFIE

(1) KOCH, Miloš a Viktor ONDRÁK. *Informační systémy a technologie*. Brno: Akademické nakladatelství CERM, 2004. ISBN 80-214-2725-6.

(2) MOLNÁR, Zdeněk. *Efektivnost informačních systémů*. 2. rozš. vyd. Praha: Grada, 2001. Management v informační společnosti. ISBN 80-247-0087-5.

(3) MOLNÁR, Zdeněk. *Moderní metody řízení informačních systémů*. V Praze: Grada, 1992. Nestůjte za dveřmi (Grada). ISBN 80-856-2307-2.

(4) GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. *Podniková informatika*. 2., přeprac. a aktualiz. vyd. Praha: Grada, 2009. Expert (Grada). ISBN 978-80-247-2615-1.

(5) SODOMKA, Petr a Hana KLČOVÁ. *Informační systémy v podnikové praxi*. 2., aktualiz. a rozš. vyd. Brno: Computer Press, 2010. ISBN 978-80-251-2878-7.

(6) DOSTÁL, Jiří. *Školní informační systémy*. Olomouc: Univerzita Palackého v Olomouci, 2011. ISBN 978-80-244-2806-2.

(7) GRASSEOVÁ, Monika, Radek DUBEC a David ŘEHÁK. *Analýza podniku v rukou manažera: 33 nejpoužívanějších metod strategického řízení*. 2. vyd. Brno: BizBooks, 2012. ISBN 978-80-265-0032-2.

(8) HALBICH, Čestmír a Dagmar BRECHLEROVÁ. *Bezpečnost informačních systémů: vybrané kapitoly*. Praha: Credit, 2003. ISBN 80-213-1090-1.

(9) MALLYA, Thaddeus. *Základy strategického řízení a rozhodování*. Praha: Grada, 2007. Expert (Grada). ISBN 978-80-247-1911-5.

(10) SCHWALBE, Kathy. *Řízení projektů v IT*. Brno: Computer Press, 2007. Kompletní průvodce (Computer Press). ISBN 978-80-251-1526-8.

(11) *ZEFIS - audit informačních systémů* [online]. Brno: Doc. Ing. Miloš Koch, CSc. [cit. 2021-01-23]. Dostupné z: https://www.zefis.cz/

(12) HENDL, Jan. *Kvalitativní výzkum: základní teorie, metody a aplikace*. Čtvrté, přepracované a rozšířené vydání. Praha: Portál, 2016. ISBN 978-80-262-0982-9.

(13) RAIS, Karel a Radek DOSKOČIL. *Risk management: studijní text pro kombinovanou formu studia*. Brno: Akademické nakladatelství CERM, 2007. ISBN 978-80-214-3510-0.

(14) *Aktuality - Portál justice* [online]. Praha: Ministerstvo spravedlnosti České republiky [cit. 23.01.2021]. Dostupné z: https://justice.cz/

(15) *ScioŠkola Brno* [online]. Brno: www.scio.cz [cit. 23.01.2021]. Dostupné z: https://brno.scioskola.cz/

(16) *ScioŠkoly - síť inovativních škol po celé ČR* [online]. Praha: www.scio.cz, s.r.o., 2020 [cit. 2020-10-25]. Dostupné z: https://scioskoly.cz/

(17) *Český statistický úřad | ČSÚ* [online]. Praha: Český statistický úřad, 2021 [cit. 2021-04-18]. Dostupné z: https://www.czso.cz/

(18) *Masarykova univerzita* [online]. Brno: Masarykova univerzita, 2021 [cit. 2021-04-18]. Dostupné z: https://www.muni.cz/

(19) *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Zlín: AION CS, 2021 [cit. 2021-04-18]. Dostupné z: https://www.zakonyprolidi.cz/

(20) *MŠMT ČR* [online]. Praha: MŠMT, 2021 [cit. 2021-04-18]. Dostupné z: https://www.msmt.cz/

(21) *Parlament České republiky, Poslanecká sněmovna* [online]. Praha: Parlament České republiky, Poslanecká sněmovna, 2021 [cit. 2021-04-18]. Dostupné z: https://www.psp.cz/

(22) *Edookit* [online]. Praha: EDOOKIT [cit. 2021-01-24]. Dostupné z: https://edookit.com/cs/

(23) VEJRAŽKA, Roman. *Edookit podrobně*. Brno, 2021.

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

a.s.	akciová společnost
BI	Business Intelligence
CI	Customer Intelligence
CPM	Critical Path Method
CRM	Customer Relationship Management
DNS	Domain Name Server
DVD	Digital Video Disc
ERP	Enterprise Resource Planning
EU	Evropská Unie
GB	Gigabyte
GDPR	General Data Protection Regulation
HDD	Hard Disk Drive
HP	Hewlett-Packard
HR	Human Resources
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IS	Informační Systém
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Informační Technologie
MIS	Management Information System
MŠ	Mateřská Škola
NATO	North Atlantic Treaty Organization
PC	Personal Computer

SLA	Service-Level Agreement
s.r.o.	společnost s ručením omezeným
SCM	Supply Chain Management
SŠ	Střední Škola
UPS	Uninterruptible Power Supply
VOŠ	Vyšší Odborná Škola
VŠ	Vysoká Škola
ZŠ	Základní Škola

SEZNAM POUŽITÝCH OBRÁZKŮ

SEZNAM POUŽITÝCH ROVNIC

SEZNAM POUŽITÝCH TABULEK

SEZNAM POUŽITÝCH GRAFŮ